

A Generic Construction of an Anonymous Reputation System and Instantiations from Lattices

Johannes Blömer ¹, Jan Bobolz ², and Laurens Porzenheim ¹ 

¹ Paderborn University, Paderborn, Germany

{bloemer, laurens.porzenheim}@upb.de

² University of Edinburgh, Edinburgh, UK (work done while at Paderborn University) jan.bobolz@ed.ac.uk

Abstract. With an anonymous reputation system one can realize the process of rating sellers anonymously in an online shop. While raters can stay anonymous, sellers still have the guarantee that they can only be reviewed by raters who bought their product.

We present the first generic construction of a reputation system from basic building blocks, namely digital signatures, encryption schemes, non-interactive zero-knowledge proofs, and linking indistinguishable tags. We then show the security of the reputation system in a strong security model. Among others, we instantiate the generic construction with building blocks based on lattice problems, leading to the first module lattice-based reputation system in the random oracle model.

1 Introduction

Reputation systems are crucial for markets to function properly. They are usually a user’s only indicator regarding the trustworthiness of a seller, or the quality of a product. Right now, in real-world reputation systems, ratings are centrally controlled (see, for example, Amazon or Yelp ratings) by the reputation system provider (Amazon/Yelp). This means that the reputation system provider has the ability to admit or deny users from the system, censor ratings, inject fake ratings, and trace all raters’ identities. Of course, this allows a malicious provider to unilaterally undermine the reputation system, e.g. by censoring inconvenient ratings or by using knowledge of user identities to retaliate against bad ratings.

Cryptographic reputation systems. A *cryptographic* reputation system is a decentralized system in which the roles and abilities of the reputation system provider

This work was partially supported by the German Research Foundation (DFG) within the Collaborative Research Centre “On-The-Fly Computing” under the project number 160364472 – SFB 901/3. Additionally, this work was partially funded by the Ministry of Culture and Science of the State of North Rhine-Westphalia.

This article is the full version of an article with the same name which appeared at Asiacrypt 2023, ©IACR 2023.

are either fully replaced by cryptographic mechanisms or at least distributed among multiple parties, with strong anonymity guarantees for users. First, a user registers (once) with the *group manager*, who is tasked with admitting users to the system (essentially to prevent Sybil attacks). Then, when the user buys a product, he receives a *rating token* from an *issuer* (e.g., the seller), certifying that the user is indeed allowed to rate the issuer (to prevent users from rating issuers they have never interacted with). Given the membership certificate from the group manager and the rating token from the issuer, the user can create a *rating signature*. We imagine that the user posts this signature to a public *reputation board*, enabling other users to view and verify the rating. The rating signature is *anonymous*, meaning that it does not reveal who, of all users who are allowed to rate that issuer, issued this particular rating (preventing retaliation against negative ratings). However, the *opener* possesses a special key to inspect signatures and reveal the user’s identity in case of misuse. Finally, even though rating signatures are otherwise anonymous to the public, anyone can efficiently check whether any two rating signatures have been created by the same user (to prevent the same user from submitting multiple ratings for the same issuer). In this setting, the role of the reputation system provider has been distributed among group manager, issuers and reputation boards. User anonymity is cryptographically guaranteed, but can be revoked by the opener. What we describe here can be seen as (a special case of) the ticket-based approach identified by [GG21].

Desirable construction types. There exists a wealth of constructions of such system in the literature (as surveyed in [GG21]), but they all work in the discrete logarithm setting. With the looming threat of quantum computers, there is a need for constructions that do not rely on the hardness of discrete logarithms and instead rely on some hardness assumption not likely broken by quantum computers, such as lattice-based assumptions. We are aware of only a single lattice-based reputation system in the literature, designed by El Kaafarani, Katsumata, and Solomon [EKS18]. We can generally distinguish generic constructions from non-generic constructions. A generic construction is a prescription how to plug together (almost) arbitrary instantiations of several basic schemes (e.g., signature schemes, encryption schemes, and non-interactive zero-knowledge proofs (NIZKs)) into a secure reputation system. So far, reputation system constructions have been non-generic, i.e. there is no formally proven way to construct reputation systems from arbitrarily instantiated basic building blocks. Even beyond the lack of an *explicit* generic construction, existing constructions are also quite specific to their (discrete logarithm / lattice) setting. For example, a natural choice for rating tokens would be for the issuer to sign the buying user’s public key (thereby giving that user the right to rate). However, in the discrete logarithm setting (e.g., [BJK15; BEJ18]), rating tokens are typically (blind) signatures on the user’s *secret key*, instead, because traditionally, it is easier to sign secret keys (which live in \mathbb{Z}_p) than public keys (which live in the group \mathbb{G}). In the lattice setting, the only known construction [EKS18] accumulates all buyers’ public keys in a Merkle hash tree, which is (relatively) efficient in the lattice set-

ting, but would be absurdly inefficient and borderline impossible to implement in the discrete logarithm setting (considering the need to prove statements in zero-knowledge about the hashes).

1.1 Our Contribution

In this paper, we give the first provably secure *generic* construction of a reputation system from digital signatures, public-key encryption, linking indistinguishable tags (LITs), and NIZKs. We formally define security properties and prove that the generic construction (and hence any concrete constructions built from it) fulfills them. Furthermore, we show that this generic construction can be reasonably instantiated in both the lattice setting and the discrete logarithm setting, unifying and drawing parallels between the two settings. In particular, this results in the first reputation system based on *module* lattices, i.e. on the hardness of module lattice problems. Our construction compares favorably in its privacy properties to the only other lattice-based construction [EKS18], as discussed later.

Generic construction. The generic construction roughly follows a paradigm similar to the sign-encrypt-prove paradigm [CS97] for group signatures, similar to [BJK15; BEJ18] (but modified to apply to both the lattice and the discrete logarithm setting). The user generates some secret key usk ; his public key is $\text{upk} = f(\text{usk})$ for some one-way function f . To join the system, the user obtains a signature ρ on his public key under the public key gmpk of the group manager. To enable rating an issuer, who we identify by his public key ipk , the user also obtains a signature τ on his public key from the issuer. Given those two signatures, the user composes a rating text rtng and encrypts his public key upk for the opener (who holds the decryption key to reveal upk in case of misuse). For technical reasons, the user also encrypts usk under a key that nobody knows the secret key for (a trick comparable to the Naor-Yung paradigm). Furthermore, the user computes a *linking indistinguishable tag* (LIT) using his secret key usk . The LIT is the gadget that will allow anyone to check whether the user has rated the same issuer twice. Then, the user uses the NIZK essentially as a signature of knowledge [CL06] to create a non-interactive proof authenticating the rating text rtng by proving, in zero-knowledge, that the ciphertexts and LIT have been computed correctly, and that his public key upk has been signed by the group manager and the issuer.

Instantiation in the discrete logarithm setting. In the discrete logarithm setting, we can use LIT tags in the random oracle model of the form $\mathcal{RO}(\text{ipk})^{\text{usk}}$ (note that this is a deterministic tag and hence enables detection of a user rating ipk twice). Because the generic construction signs *public* keys, we use a structure-preserving signature as the signature scheme. Unsurprisingly, encryption can be accomplished with ElGamal and the NIZKs can be instantiated with Schnorr-style protocols together with the Fiat-Shamir heuristic. More details can be found in Section 5.1.

Instantiation with lattices. The instantiation with lattices is more difficult given that the ecosystem for privacy constructions is less mature than in the discrete logarithm setting. We need to instantiate the encryption scheme, the signature scheme, the NIZK, and the linking indistinguishable tag. For more efficiency and flexibility when setting parameters, we generally consider the *module* lattice setting. For the encryption scheme, the typical choice is between primal and dual Regev encryption (i.e. between putting the LWE error into the public key or into ciphertexts). Primal Regev is more suitable for proving statements about encryptions in zero-knowledge, since there is no added error in the ciphertext, which is why we choose it for the instantiation. In particular, we use the verifiable encryption scheme described by [LNP22b]. For the NIZK, we choose [LNP22b], which has the advantage of supporting efficient vector shortness proofs without slack, but is in the random oracle model. We use this feature to efficiently prove knowledge of, for example, a valid [DM14] signature. This NIZK also interfaces well with the other schemes chosen to instantiate the generic construction. Finally, we require a linking indistinguishable tag. We use a tag similar to those of [BE17; EKS18], which can be seen as the lattice equivalent of DLOG-based tags mentioned above. To build a LIT tag \mathbf{t} in the lattice setting, [EKS18] use an LWE secret as the secret key, hash the message μ with the random oracle, and choose an error \mathbf{e} to build an LWE sample from it, i.e. $\mathbf{t}^t = \mathbf{s}^t \cdot \mathcal{R}\mathcal{O}(\text{ipk}) + \mathbf{e}^t$. Linking works because if one tags the same message with the same secret key, the difference of the two tags is the difference of the two errors. Thus, the difference of two tags is short, iff they should link. [EKS18] show the security of their tag under the first-are-errorless LWE assumption, a variant of LWE where the first few samples of an LWE oracle do not contain any error. When instantiating the LIT, this costs them some efficiency, so we modify their construction to show our tag secure under the Module LWE assumption. We also introduce some new security notions for LITs in order to interface better with our generic construction.

There are several signature schemes based on lattice assumptions. However, we require one that plays nicely with zero-knowledge proofs, for example the signature should not rely on random oracles. Thus, a first idea would be to use the signatures of [Lib+16] or [JRS23], as they are designed to be compatible with current lattice-based proof systems. However, [Lib+16] present a construction based on unstructured lattices, which is too inefficient compared to a construction from structured lattices. Furthermore, their construction inherently uses a chameleon hash to achieve adaptive security, which increases the complexity of a proof of possession of a signature. On the other hand, [JRS23] construct both a stateful ℓ -time signature and a stateless ℓ -time signature that are both directly adaptively secure. However, the former does not fit our generic construction, which requires a stateless signature scheme without a limit on the signature queries. For the latter we can argue that we can use it in our generic construction despite the ℓ -time restriction, but it suffers from a large reduction loss. Another candidate is the stateless signature scheme of [DM14]. Like the other two signatures, it is a tag-based signature scheme and a variant of sig-

natures by [Boy10], but is based on ideal lattices. [DM14] show their signature to be non-adaptively secure and transform it to adaptive security by employing chameleon hashes. We instead show in Appendix B that the signature of [DM14] is already adaptively secure by using a proof technique as in [LSS14]. However, the signature scheme of [DM14] also suffers from a high reduction loss similar to the stateless variant of [JRS23], since they use the same proof technique. Another possible signature scheme, especially when optimizing for signature size, is the one by [Boo+23]. They design a credential system, which can be based on one of several new lattice assumptions, such as Int-NTRU-ISIS_f. This credential system implies a signature scheme that we can use in our generic construction. For the signature schemes of [JRS23; Boo+23] we later give rough estimates of the size of a signature of a rating. For details, see Section 5.

Stateful reputation system. We also discuss a stateful variant of our generic construction of a reputation system in Section 5, which is limited to ℓ users. The stateful variant works the same way as the stateless construction except for using stateful signatures as building blocks instead and having a fixed maximum number of users. The security proofs of the stateless generic construction can easily be adapted to apply to the stateful variant. Then, we can instantiate the stateful generic construction with the same schemes as discussed before, except for using the stateful signature scheme of [JRS23]. Since their stateful scheme is more efficient than their stateless variant, this also improves the efficiency of the reputation system instantiation.

1.2 Related Work

Reputation system constructions. Building reputation systems in the discrete logarithm setting is well-understood, with a wealth of papers with a variety of construction strategies and features. A good discussion can be found in the survey of Gurtler and Goldberg [GG21]. Closest to our generic construction are [BJK15; BEJ18], they are not quite instantiations of our generic construction, but they follow a similar paradigm (changes are mostly due to the fixed discrete logarithm setting in those papers, such as the usage of blind signatures to avoid signing public keys). Other papers, such as [LM19; BSS10], offer some form of privacy for issuers. In our construction, the issuer is known to all parties. We leave extensions, which offer some privacy to issuers, to future work and note that the techniques used here carry over to more complex scenarios. Another line of research considers reputation systems in a blockchain context, as surveyed by Hasan, Brunie, and Bertino [HBB23]. Those systems usually aim for trustlessness, i.e. ideally *no* party has to be trusted, but trust is distributed and backed by incentives throughout the blockchain network. Our system makes some trust assumptions, e.g., if group manager and issuer collude, we cannot prevent Sybil attacks. We do not model any reputation board party mentioned by [HBB23], which stores the rating signatures, but note that it can be realized by a public ledger, ensuring that ratings are not censored or deleted.

Lattice-based group signatures and credential systems. One way to construct a reputation system is to take some group signature as base and to modify it such that linking is possible [EKS18; BJK15; BEJ18]. This works because the notion of group signatures is closely related to anonymous reputation systems; one can view reputation systems as a group of group signatures. Both want to protect the anonymity of users inside a group or system, where the users authenticate messages, while a privileged opener is able to de-anonymize users. Therefore, we can explore existing lattice-based group signatures as potential bases for a lattice-based reputation system. One example is the group signature of [Lin+17], which [EKS18] used to construct their reputation system, as explained later in more detail.

Another potential group signature to build a reputation system from is the one of [Bos+20], which uses the sign-encrypt-proof paradigm. They employ the Aurora SNARK [Ben+19] for their proofs, which has the advantage of no slack and very small proofs. However, the computation time for the proofs required by the group signature seems to be too high, as [Bos+20] explain.

In their paper on very efficient NIZKs with no slack, [Lyu+21] also present a group signature scheme, which is based on the constructions of [PLS18; Lyu+21]. While this scheme promises very short signatures, their group signature is static, i.e. the group does not change. This does not match our dynamic model of a reputation system. Furthermore, [Lyu+21] model their user identities as single ring elements of a special set, which they sign to let the user join the group. However, in our construction we need to be able to sign the public keys of the LIT scheme, which generally do not fall into this special set.

Another group signature on which one could base a reputation system is the one by [Lin+18]. They also follow the sign-encrypt-proof paradigm, and concretely use the signatures of [DM14], an encryption scheme by [LPR13b] transformed to CCA security similar to the Naor-Yung paradigm and some Stern-like proof system. This group signature uses the same signature scheme and a similar encryption scheme as building blocks as we do in our first instantiation of the reputation system (note that we use different NIZKs).

Instead of basing the construction of a reputation system on some group signature, one can also look at credential system, as they are another privacy-focused primitive related to reputation systems. Two possible constructions are the systems from [JRS23] and [Boo+23]. The idea of both credential systems is that they construct a blind signature, which they use to (blindly) sign some attributes, i.e. create a credential over the attributes. To sign a message, they prove possession of a credential in zero-knowledge. Thus, the idea of their constructions is different to our generic construction, which does not need a blind signature.

Lattice-based reputation systems. To the best of our knowledge, the only other construction of a reputation system that is based on lattices is the construction of [EKS18]. The idea for their construction is to start with the group signature from [Lin+17] and view the reputation system as a group of group signatures. For each item that can be rated, the group manager sets up a separate group

signature via a hash-based accumulator that is a Merkle-tree of all public keys of users who may rate the item. To create a rating a user encrypts his identity, creates a tag with a LIT and proves in zero-knowledge that he encrypted and tagged correctly as well as that his public key, for which he knows the secret key, is contained in the Merkle-tree.

A drawback of their model is that there are no issuers, instead there is a single group manager who manages everything. This gives the single group manager more power in a setting where there are different people to be rated, where these people need to trust the single group manager to work honestly. By separating the group manager from issuers, we can also split up their power, allowing for a more fine-grained approach of modelling trust. This is reflected in our security model. Additionally our security model offers a slightly stronger corruption model, except for requiring the opener to be honest (cf. Section 4.1).

Another drawback of the construction of [EKS18] is that due to it relying on public Merkle-trees, there exists a public record of all users who can rate an item. While this does not contradict any formal security notion, in practice it is undesirable that the whole purchase history of all users is publicly available and a construction not exhibiting this issue is preferable. Our construction prevents this drawback by using signatures instead of a Merkle-tree to add users to the group. Obviously, even in our setting malicious issuers can always share the purchase history of users who bought from them with other people, but this is unpreventable. However, [EKS18] *requires* their group manager to publish this information in order for the system to work. Furthermore, due to their usage of first-are-errorless LWE for the LIT as mentioned before and their usage of Stern-like proofs, the construction of [EKS18] is less efficient than ours.

The advantage that the construction of [EKS18] has over our construction is that they can assume the opener to be corrupt in every security notion but anonymity, while our construction needs the opener to be honest-but-curious. [EKS18] achieve this requirement by introducing a **Judge** algorithm with which one can publicly verify that the opener worked correctly. We note that it is straight-forward to add **Judge** to our generic construction and our instantiations, but we omit it for better readability.

2 Preliminaries

We denote drawing some x uniformly from a set S by $x \leftarrow S$. We overload notation and denote by $x \leftarrow D$ sampling x from a distribution D . If $A(y)$ is a (probabilistic polynomial time (ppt)) algorithm, $x \leftarrow A(y)$ denotes sampling x from the output distribution of A on input y . $[A(y)]$ denotes the set of possible outcomes of a ppt A on input y . We denote the random oracle as \mathcal{RO} .

We denote scalars as lowercase letters a , column vectors as bold lowercase letters \mathbf{a} and matrices as bold uppercase letters \mathbf{A} . By \mathbf{I}_c we denote the identity matrix of dimension $c \times c$. If the dimensions are clear from the context, we may only write \mathbf{I} . The same holds for $\mathbf{0}$, by which we denote the vector or matrix

consisting of only zeroes. For the norm $\|\mathbf{a}\|$ of a vector we use the euclidian norm unless specified otherwise. We denote the infinity norm of a vector by $\|\mathbf{a}\|_\infty$.

Unless otherwise specified, let $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$ with $n \geq 16$ being a power of two and let $q > 16$ and $q = 3, 5 \pmod{8}$. Let $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. With such a q , \mathcal{R}_q splits into $\mathcal{R}_q \cong \mathbb{F}_{q^{n/2}} \times \mathbb{F}_{q^{n/2}}$, where $\mathbb{F}_{q^{n/2}}$ denotes the field with $q^{n/2}$ elements, which we use for some results, e.g. Lemma 1. We represent elements of \mathcal{R}_q as vectors over \mathbb{Z}_q^n . In general, we use the coefficient embedding $\theta : \mathcal{R}_q \rightarrow \mathbb{Z}_q^n$, since for the \mathcal{R} we use the canonical embedding is the same as the coefficient embedding up to a factor of \sqrt{n} [JRS23]. Define $\mathcal{R}_2 = \theta^{-1}(\{0, 1\}^n)$ and $\mathcal{R}_{\pm 1} = \theta^{-1}(\{-1, 0, 1\}^n)$. By \tilde{x} we refer to the constant term of some polynomial $x \in \mathcal{R}$.

For CPA security of an encryption scheme and EUF-CMA security of a signature scheme we use the standard definitions. See Appendix E for definitions.

2.1 Problems on Lattices

Definition 1 (MLWE). *Let $q > 2$ and $k > 0$. Let \mathcal{R} be a ring and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let χ be a distribution over \mathcal{R}_q . For a secret $\mathbf{s} \in \mathcal{R}_q^k$, the Module Learning With Errors (MLWE) $A_{\mathbf{s}}$ distribution is defined as choosing $\mathbf{a} \leftarrow \mathcal{R}_q^k$ and $e \leftarrow \chi$, computing $b = \mathbf{s}^t \mathbf{a} + e \pmod{q}$, and outputting (\mathbf{a}, b) .*

The MLWE problem $\text{MLWE}_{q, \mathcal{R}, k, \chi}$ is then defined as distinguishing between $A_{\mathbf{s}}$ for a secret $\mathbf{s} \leftarrow \mathcal{R}_q^k$ and the uniform distribution over \mathcal{R}_q^{k+1} .

It can be useful to group the \mathbf{a}_i from m samples together as the column vectors of a matrix $\mathbf{A} \in \mathcal{R}_q^{k \times m}$ and the b_i as the entries of a vector $\mathbf{b} \in \mathcal{R}_q^m$, such that we have $\mathbf{s}^t \mathbf{A} + \mathbf{e}^t = \mathbf{b}^t$ for some error vector $\mathbf{e} \in \mathcal{R}_q^m$.

There exists an alternative version of the MLWE problem, where the secret is not sampled uniformly from \mathcal{R}_q , but instead sampled as $\mathbf{s} \leftarrow \chi^k$. This is called the *normal form* of MLWE. The described MLWE problems are decisional problems. There exist computational variants, where the goal is to compute the secret \mathbf{s} , given samples from the respective MLWE distribution. This is called the (normal form) *search* MLWE problem $\text{sMLWE}_{q, \mathcal{R}, k, \chi}$.

In some cases, we need to set the parameters of the normal form MLWE problem in such a way that the secret used to create a set of m samples is unique, meaning that with overwhelming probability there is no other secret and error vector that could produce the samples.

Lemma 1 (Short MLWE secrets are unique). *Let $q \neq 2$ be a prime with $q = 3, 5 \pmod{8}$ (or $q = 1 \pmod{2n}$), $k > 0$, $n > 16$ be a power of 2, $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$. Let $B_\beta = \{e \in \mathcal{R}_q : \|e\|_\infty \leq \beta\}$. Let $\Delta \geq 0$ such that $2\beta + \Delta < q^{1/4}$. Then, there exists an m and a negligible function negl such that*

$$\Pr \left[\begin{array}{l} \exists (\mathbf{s}, \mathbf{s}', \mathbf{e}, \mathbf{e}') \in (B_\beta^k)^2 \times (B_\beta^m)^2 \\ \text{with } \mathbf{s} \neq \mathbf{s}' \wedge \|\mathbf{b}\|_\infty \leq \Delta \end{array} : \begin{array}{l} \mathbf{A} \leftarrow \mathcal{R}_q^{k \times m} \\ \mathbf{b}^t = (\mathbf{s} - \mathbf{s}')^t \mathbf{A} + (\mathbf{e} - \mathbf{e}')^t \end{array} \right] \leq \text{negl}(n).$$

The proof can be found in Appendix A.

2.2 NIZKs

We model non-interactive zero-knowledge proof systems in the random oracle model. This is because when instantiating our generic construction of a reputation system, the NIZKs we use are in the random oracle model. The generic construction itself and the security proofs, however, do not make use of the random oracle model. There, it would suffice to model NIZKs without a random oracle by simply removing it from the syntax and security models.

Definition 2 (NIZK). *A non-interactive proof system (NIZK) for a relation \mathfrak{R} in the random oracle model is defined as a triple $\Pi_{\text{NIZK}} = (\text{Setup}, \mathcal{P}, \mathcal{V})$ of ppt algorithms:*

- $\text{Setup}(1^n)$ outputs a common reference string crs .
- $\mathcal{P}^{\mathcal{RO}(\cdot)}(\text{crs}, x, w, m)$ given instance x , witness w , and a message m , outputs a proof π .
- $\mathcal{V}^{\mathcal{RO}(\cdot)}(\text{crs}, x, m, \pi)$ outputs a bit b .

To simplify notation, we sometimes omit the random oracle $\mathcal{RO}(\cdot)$, but assume implicitly that the prover and verifier have access to it. We say that the NIZK is correct, if for all $(x, w) \in \mathfrak{R}$ and $m \in \{0, 1\}^*$, we have that

$$\Pr[\mathcal{V}(\text{crs}, x, m, \mathcal{P}(\text{crs}, x, w, m)) : \text{crs} \leftarrow \text{Setup}(1^n)] = 1.$$

For a relation \mathfrak{R} , $L_{\mathfrak{R}} = \{x \mid \exists w : (x, w) \in \mathfrak{R}\}$ is the language associated with \mathfrak{R} . The message m is additional data bound to the proof (e.g., including m in a Fiat-Shamir hash). Its role can be observed in Definition 6.

In order to display the relation \mathfrak{R} that is proven, we will use the following notation for proofs.

Definition 3. *We denote the generation of a proof $\pi \leftarrow \mathcal{P}(\text{crs}, x, w, m)$ by*

$$\pi \leftarrow \text{NIZK}\{x; w; \mathfrak{R}(x, w)\}(m),$$

where \mathcal{P} is from a non-interactive proof system Π_{NIZK} for the relation \mathfrak{R} . We say “Verify π ” to mean checking that $\mathcal{V}(\text{crs}, x, m, \pi) = 1$ and we say “ π verifies” or “ π is valid” if $\mathcal{V}(\text{crs}, x, m, \pi) = 1$ holds.

With respect to security, we require the NIZK to be zero-knowledge (i.e. proofs can be simulated without a witness), sound (i.e. one cannot prove false statements), simulation-sound (i.e. one cannot prove false statements, even in the presence of simulated proofs), and straight-line extractable (i.e. there exists an extractor that can efficiently compute a witness from a valid proof without rewinding). These definitions are standard, we list them below, starting with zero-knowledge.

Definition 4 (Zero-Knowledge). *A NIZK Π is zero-knowledge if there exists a simulator \mathcal{S} consisting of three ppt algorithms $\mathcal{S} = (\mathcal{S}.\text{Setup}, \mathcal{S}.\mathcal{RO}, \mathcal{S}.\text{Sim})$ such that for all ppt \mathcal{A} there exists a negligible function negl such that,*

$$\text{Adv}_{\Pi, \mathcal{A}}^{\text{ZK}}(n) = \left| \frac{\Pr[\mathcal{A}^{\mathcal{P}(\text{crs}, \cdot, \cdot), \mathcal{RO}(\cdot)}(1^n, \text{crs}) = 1 : \text{crs} \leftarrow \text{Setup}(1^n)]}{\Pr[\mathcal{A}^{\text{Sim}(\cdot, \cdot, \cdot), \mathcal{S}.\mathcal{RO}(\cdot)}(1^n, \text{crs}) = 1 : \text{crs} \leftarrow \mathcal{S}.\text{Setup}(1^n)]} \right| \leq \text{negl}(n)$$

where \mathcal{RO} denotes a random oracle. The oracle $\text{Sim}(x, w, m)$ checks if $(x, w) \in \mathfrak{R}$ and if so, runs $\mathcal{S}.\text{Sim}(x, m)$. We assume that \mathcal{S} is stateful, i.e. it implicitly keeps state between invocations of $\mathcal{S}.\text{Setup}$, $\mathcal{S}.\mathcal{RO}$, and $\mathcal{S}.\text{Sim}$.

We give the simulator two advantages beyond a regular prover that should allow it to efficiently simulate proofs without a witness: (1) $\mathcal{S}.\text{Setup}$ generates crs and that process can yield a trapdoor that \mathcal{S} stores in its state. (2) \mathcal{S} answers the random oracle queries of \mathcal{A} with $\mathcal{S}.\mathcal{RO}(\cdot)$, so \mathcal{S} can program random oracle answers.

The second requirement we have is soundness, which states it is hard for an adversary to prove a false statement.

Definition 5 (Soundness). *We say that a NIZK Π is sound if for all ppt \mathcal{A} , there is a negligible function negl such that*

$$\text{Adv}_{\Pi, \mathcal{A}}^{\text{Snd}}(n) = \Pr \left[\begin{array}{l} \mathcal{V}^{\mathcal{RO}(\cdot)}(\text{crs}, x, m, \pi) = 1 \wedge x \notin L_{\mathfrak{R}} : \\ \text{crs} \leftarrow \text{Setup}(1^n), (x, m, \pi) \leftarrow \mathcal{A}^{\mathcal{RO}(\cdot)}(1^n, \text{crs}) \end{array} \right] \leq \text{negl}(n)$$

Next, we require simulation soundness, i.e. even given access to an oracle creating simulated proofs (potentially for false statements), it is hard to compute an accepting proof for a wrong (not-queried) statement x .

Definition 6 (Simulation soundness). *Let $\Pi = (\text{Setup}, \mathcal{P}, \mathcal{V})$ be a zero-knowledge NIZK, with simulator \mathcal{S} as in Definition 4. We say that a NIZK Π is simulation-sound if for all ppt \mathcal{A} , there exists a negligible function negl with*

$$\text{Adv}_{\Pi, \mathcal{A}}^{\text{SS}}(n) = \Pr \left[\begin{array}{l} \mathcal{V}^{\mathcal{S}.\mathcal{RO}(\cdot)}(\text{crs}, x, m, \pi) = 1 \\ \wedge x \notin L_{\mathfrak{R}} \\ \wedge \mathcal{A} \text{ has not queried } \mathcal{S}.\text{Sim}(x, m) \end{array} : \begin{array}{l} \text{crs} \leftarrow \mathcal{S}.\text{Setup}(1^n), \\ (x, m, \pi) \leftarrow \mathcal{A}^{\mathcal{S}.\text{Sim}(\cdot, \cdot), \mathcal{S}.\mathcal{RO}(\cdot)}(1^n, \text{crs}) \end{array} \right] \leq \text{negl}(n)$$

Note that, as usual, \mathcal{A} may even query $\mathcal{S}.\text{Sim}(x, m)$ for $x \notin L$. The simulation soundness property is sometimes understood to imply non-malleability of the proof π , i.e. defined with the condition “ π has not been output by $\mathcal{S}.\text{Sim}(x, m)$ ” instead of “ \mathcal{A} has not queried $\mathcal{S}.\text{Sim}(x, m)$ ”. We use the weaker condition here, which corresponds to the fact that we do not consider immaterial changes to rating signatures (e.g., re-randomization with no change to the rating text or the rated party) an attack (see, for example, Definition 18).

Finally, we require straight-line extractability.

Definition 7 (Straight-line extractability). *Let $\Pi = (\text{Setup}, \mathcal{P}, \mathcal{V})$ be a NIZK. We say that Π is a straight-line extractable proof of knowledge if there are ppt algorithms $\mathcal{E}_0, \mathcal{E}_1$ such that for all ppt $\mathcal{A}_0, \mathcal{A}_1$, there exist negligible functions $\text{negl}_0, \text{negl}_1$ such that*

$$\text{Adv}_{\Pi, \mathcal{A}_0}^{\text{PoK}_0}(n) = \left| \begin{array}{l} \Pr[\mathcal{A}_0(1^n, \text{crs}) = 1 : \text{crs} \leftarrow \text{Setup}(1^n)] \\ - \Pr[\mathcal{A}_0(1^n, \text{crs}) = 1 : (\text{crs}, td) \leftarrow \mathcal{E}_0(1^n)] \end{array} \right| \leq \text{negl}_0(n)$$

and

$$\text{Adv}_{\Pi, \mathcal{A}_1}^{\text{PoK}_1}(n) = \Pr \left[\begin{array}{l} \mathcal{V}^{\mathcal{RO}}(\text{crs}, x, m, \pi) = 1 \\ \wedge (x, w) \notin \mathfrak{R} \end{array} : \begin{array}{l} (\text{crs}, td) \leftarrow \mathcal{E}_0(1^n), \\ (x, m, \pi) \leftarrow \mathcal{A}_1(1^n, \text{crs}), \\ w \leftarrow \mathcal{E}_1(td, x, m, \pi) \end{array} \right] \leq \text{negl}_1(n)$$

In the random oracle model, \mathcal{E}_1 gets the list of random oracle queries that \mathcal{A} made as additional input.

We give the extractor the advantage of setting up crs (allowing it to embed a trapdoor td) and, in the random oracle model, of observing the random oracle queries of \mathcal{A} (as in [Fis05a]). The extractor does not have any ability to rewind \mathcal{A} , so extraction through rewinding is not an option. Note that in this security definition, we do not give \mathcal{A} access to simulated proofs.

Later on, to instantiate the reputation system based on lattices, we want to use NIZKs over the following relation.

Definition 8. Let $q > 0$, \mathcal{R} a ring, $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let $\phi, \phi_{eval}, d, e, v_d, v_e, m_1, \ell$ and k_{bin} be non-negative. Let $\psi : \mathcal{R} \rightarrow \mathcal{R}, x \mapsto x(X^{-1})$ be an automorphism. Let

- $f_i : \mathcal{R}_q^{2(m_1+\ell)} \rightarrow \mathcal{R}_q$ be a quadratic function for $i \in [\phi]$,
- $F_i : \mathcal{R}_q^{2(m_1+\ell)} \rightarrow \mathcal{R}_q$ be an evaluation function for $i \in [\phi_{eval}]$,
- $\mathbf{D}_i \in \mathcal{R}_q^{k_i \times 2(m_1+\ell)}, \mathbf{u}_i \in \mathcal{R}_q^{k_i}$ for $i \in [v_d]$,
- $\mathbf{E}_i \in \mathcal{R}_q^{p_i \times 2(m_1+\ell)}, \mathbf{v}_i \in \mathcal{R}_q^{p_i}$ for $i \in [v_e]$,
- $(\beta_i^{(d)})_{i \in [v_d]}, (\beta_i^{(e)})_{i \in [v_e]}$ be some bounds,
- $\mathbf{E}_{bin} \in \mathcal{R}_q^{k_{bin} \times 2(m_1+\ell)}$ and $\mathbf{v}_{bin} \in \mathcal{R}_q^{k_{bin}}$.

Call the combination of these parameters pp . Define the relation \mathfrak{R}^R to consist of pairs (pp, \mathbf{s}) with $\mathbf{s} = (\mathbf{s}_1, \psi(\mathbf{s}_1), \mathbf{m}, \psi(\mathbf{m})) \in \mathcal{R}_q^{2m_1} \times \mathcal{R}_q^{2\ell}$, such that the following conditions hold:

$$\begin{aligned} \forall 1 \leq i \leq \phi, f_i(\mathbf{s}) &= 0 \\ \forall 1 \leq i \leq \phi_{eval}, \tilde{F}_i(\mathbf{s}) &= 0 \\ \forall 1 \leq i \leq v_d, \|\mathbf{D}_i \mathbf{s} - \mathbf{u}_i\|_\infty &\leq \beta_i^{(d)} \\ \forall 1 \leq i \leq v_e, \|\mathbf{E}_i \mathbf{s} - \mathbf{v}_i\| &\leq \beta_i^{(e)} \\ \mathbf{E}_{bin} \mathbf{s} - \mathbf{v}_{bin} &\in \{0, 1\}^{dk_{bin}} \end{aligned}$$

Recall that the notation $\tilde{F}_i(\mathbf{s})$ denotes the constant term of polynomial $F_i(\mathbf{s})$.

Lemma 2 ([LNP22b]). *There exists a NIZK for relation \mathfrak{R}^R that is zero-knowledge and simulation-sound in the random oracle model.*

While [LNP22b] only claim soundness instead of simulation-soundness, their analysis ([LNP22a, Appendix B], based on [AFK22]) applies verbatim to simulation-soundness. This is because to argue soundness for a proof π for statement x and message m , one considers only random oracle queries of the form $\mathcal{H}(\text{pp}, x, m, \dots)$.

Simulated proofs for $(x', m') \neq (x, m)$, in contrast, are only concerned with random oracle queries of the form $\mathcal{H}(\mathbf{pp}, x', m', \dots)$. Hence programming the random oracle for $\mathbf{pp}, x', m', \dots$ does not interfere with the soundness analysis at all. We can effectively imagine that the simulator and the soundness proof use two independent random oracles.

We also want the NIZK to be straight-line extractable. For this, we use Katsumata’s transform [Kat21] as shown in [Boo+23]. Their notion of multi-proof extractability implies our straight-line extractability.

Corollary 1 ([LNP22b],[Kat21],[Boo+23]). *There exists a NIZK for relation \mathfrak{R}^R that is zero-knowledge and simulation-sound and straight-line extractable in the random oracle model.*

3 Linking Indistinguishable Tags

A building block we need are *linking indistinguishable tags* (LIT). The idea of such a scheme is that one can compute a tag for a given message with a secret key. An adversary should not be able to tell which secret key was used to create the tag. However, if one tags the same message twice, i.e. with the same secret key, anyone can discover this by linking the tags. There also exists a function f from which we can compute a public key $\mathbf{pk} = f(\mathbf{sk})$. We typically require f to be a one-way function implicitly. This public key is not used in the scheme itself, but can be used in conjunction with other primitives. The formal model looks as follows.

Definition 9. *A linking indistinguishable tags scheme consists of a function f and the following ppt algorithms:*

- $\text{KeyGen}(1^n)$: On input a security parameter n , it outputs a secret \mathbf{sk} .
- $\text{Tag}(\mathbf{sk}, \mu)$: On input a secret key \mathbf{sk} and a message μ , it outputs a tag t .
- $\text{Vrfy}(\mathbf{sk}, \mu, t)$: On input a secret key \mathbf{sk} , a message μ and a tag t , it outputs a bit b .
- $\text{Link}(\mu, t_0, t_1)$: On input a message μ and two tags t_0, t_1 , it outputs a bit b .

We require that a LIT is correct. This is the case if for all security parameters n , all \mathbf{sk} output by $\text{KeyGen}(1^n)$, all messages μ , all tags t_0, t_1 output by $\text{Tag}(\mathbf{sk}, \mu)$, we have that $\text{Vrfy}(\mathbf{sk}, \mu, t_0) = 1$ and $\text{Link}(\mu, t_0, t_1) = 1$.

The first security requirement is tag-indistinguishability. In this indistinguishability game an adversary has to decide which of two secrets was used to create the challenge, while having access to tag oracle for these secrets. We define the oracle $\text{Tg}(c, \mu)$ to return t if there exists some $(c, \mu, t) \in Q$. Else, we return $t \leftarrow \text{Tag}(\mathbf{sk}_c, \mu)$ and add (c, μ, t) to Q .

$\text{Anon}_{\Pi, \mathcal{A}, b}^{LIT}(n)$
1 : $\text{sk}_0, \text{sk}_1 \leftarrow \text{KeyGen}(1^n)$
2 : $\text{pk}_i = f(\text{sk}_i), i \in \{0, 1\}$
3 : $\mu^* \leftarrow \mathcal{A}^{\text{Tg}(\cdot, \cdot)}(\text{pk}_0, \text{pk}_1)$
4 : $t^* \leftarrow \text{Tag}(\text{sk}_b, \mu^*)$
5 : $b' \leftarrow \mathcal{A}^{\text{Tg}(\cdot, \cdot)}(t^*)$
6 : If μ^* was queried, output 0, else output b' .

Definition 10. A LIT Π has tag-indistinguishability, if there exists a negligible function negl such that for all ppt adversaries \mathcal{A} it holds that

$$\text{Adv}_{\Pi, \mathcal{A}}^{LIT \text{Anon}}(n) := \left| \Pr[\text{Anon}_{\Pi, \mathcal{A}, 0}^{LIT}(n) = 1] - \Pr[\text{Anon}_{\Pi, \mathcal{A}, 1}^{LIT}(n) = 1] \right| \leq \text{negl}(n).$$

The second security requirement is linkability. This asks that no adversary can produce two secret key tag pairs and a message, such that the secret key tag pairs are valid for the message, while the tags do not link. In comparison to the security model of [EKS18], we generalize our security model for linkability and allow the adversary to output two different secret keys, but they must map to the same public key.

$\text{Linkable}_{\Pi, \mathcal{A}}^{LIT}(n)$
1 : $(\text{sk}_0, \text{sk}_1, \mu, t_0, t_1) \leftarrow \mathcal{A}(1^n)$
2 : If $f(\text{sk}_0) \neq f(\text{sk}_1)$ or $\exists i \in \{0, 1\} : \text{Vrfy}(\text{sk}_i, \mu, t_i) = 0$, return 0.
3 : If $\text{Link}(\mu, t_0, t_1) = 0$, output 1.

Definition 11. A LIT Π has linkability if there exists a negligible function negl such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{Linkable}_{\Pi, \mathcal{A}}^{LIT}(n) = 1] \leq \text{negl}(n).$$

Another security requirement, unforgeability, is similar to the requirement for a one-way function. It requires that no adversary is able to produce a secret key, message and valid tag, such that the tag links to another valid tag. For that, we need a tag oracle QTg , that on input (sk, μ) returns t if there exists $(\mu, t) \in \mathcal{Q}$. Else it computes $t \leftarrow \text{Tag}(\text{sk}, \mu)$, adds (μ, t) to \mathcal{Q} and returns t .

$\text{Forge}_{\Pi, \mathcal{A}}^{LIT}(n)$
1 : $\mathcal{Q} = \emptyset$
2 : $\text{sk} \leftarrow \text{KeyGen}(1^n), \text{pk} = f(\text{sk})$
3 : $(\text{sk}^*, \mu, t^*) \leftarrow \mathcal{A}^{\text{QTg}(\text{sk}, \cdot)}(\text{pk})$
4 : If $\text{Vrfy}(\text{sk}^*, \mu, t^*) = 0$, output 0.
5 : If $\exists (\mu, t) \in \mathcal{Q}$ such that $\text{Link}(\mu, t, t^*) = 1$, output 1.

Definition 12. A LIT Π is unforgeable, if there exists a negligible function negl such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{Forge}_{\Pi, \mathcal{A}}^{\text{LIT}}(n) = 1] \leq \text{negl}(n).$$

The last requirement for LIT schemes is non-invertability. This asks that an adversary is not able to find a secret key to given public key, while having access to a tag oracle.

$\text{Invert}_{\Pi, \mathcal{A}}(n)$
1 : $\text{sk} \leftarrow \text{KeyGen}(1^n)$
2 : $\text{pk} = f(\text{sk})$
3 : $\text{sk}' \leftarrow \mathcal{A}^{\text{QTg}(\text{sk}, \cdot)}(\text{pk})$
4 : If $\text{pk} = f(\text{sk}')$, output 1.

Here QTg is defined as before.

Definition 13. A LIT Π has non-invertability, if there exists a negligible function negl such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{Invert}_{\Pi, \mathcal{A}}(n) = 1] \leq \text{negl}(n).$$

Construction Based on Module Lattices Given the formal model of a LIT, we now want to construct a LIT based on module lattices of rank k . When we later use the LIT in our reputation system, we only need $k = 1$, in which case the security assumption for the LIT reduces to ideal lattices. The LIT may be of independent interest, so we construct it with general k .

The idea for the construction is that a public key is simply a batch of MLWE samples for some secret \mathbf{s} . A tag on a message μ is the second component of another batch of MLWE samples, i.e. $\mathbf{t}^t = \mathbf{s}^t \mathbf{A}_\mu + \mathbf{e}^{tt}$, for the same secret \mathbf{s} and some different error \mathbf{e}' , where we define $\mathbf{A}_\mu = \mathcal{RO}(\mu)$. This way, if we tag the same message twice, \mathbf{A}_μ is the same for both tags, and the difference of the two tags is equal to the difference of the two errors. Since this is short, we can detect that the tags were created for the same message.

Construction 14. Let $m, k > 0$. Let $\beta < 2^{-\frac{n}{mk} + \frac{n}{2k} \log(q) - 3}$. Let χ be a distribution over \mathcal{R}_q . Construct the LIT Π_{LIT} consisting of the following algorithms:

- $\text{KeyGen}(1^n)$: Choose $\mathbf{s} \leftarrow \chi^k$, $\mathbf{e} \leftarrow \chi^m$. Set $\text{sk} = (\mathbf{s}, \mathbf{e})$.
- $\text{Tag}(\text{sk}, \mu)$: Compute $\mathbf{A}_\mu = \mathcal{RO}(\mu) \in \mathcal{R}_q^{k \times m}$ and $\mathbf{e}' \leftarrow \chi^m$. Output $\mathbf{t}^t = \mathbf{s}^t \mathbf{A}_\mu + \mathbf{e}^{tt}$.
- $\text{Vrfy}(\text{sk}, \mu, \mathbf{t})$: Compute $\mathbf{A}_\mu = \mathcal{RO}(\mu) \in \mathcal{R}_q^{k \times m}$. If $\|\mathbf{t} - (\mathbf{s}^t \mathbf{A}_\mu)^t\|_\infty < \beta$ and $\|\mathbf{s}\|_\infty \leq \beta$, output 1.
- $\text{Link}(\mu, \mathbf{t}_0, \mathbf{t}_1)$: If $\|\mathbf{t}_0 - \mathbf{t}_1\|_\infty < 2\beta$, output 1.
- $f = f_{\mathbf{A}}$ for $\mathbf{A} \leftarrow \mathcal{R}_q^{k \times m}$, $f_{\mathbf{A}}(\text{sk}) = (\mathbf{s}^t \mathbf{A} + \mathbf{e}^t)^t$

The construction is correct, if we have that $\Pr[\|x\|_\infty \leq \beta : x \leftarrow \chi]$ with overwhelming probability.

Lemma 3. *The LIT Π_{LIT} has tag-indistinguishability (Definition 10) in the random oracle model, if normal form $\text{MLWE}_{q,\mathcal{R},k,\chi}$ is hard.*

This can be proven by proving that $\text{Anon}_{\Pi_{\text{LIT}},\mathcal{A},0}^{\text{LIT}}(n)$ is indistinguishable from a game where the challenge tag t^* is generated uniformly at random, which is possible using the indistinguishability of the MLWE distribution from the uniform distribution. Then, one does the same for $\text{Anon}_{\Pi_{\text{LIT}},\mathcal{A},1}^{\text{LIT}}(n)$, from which we can see that the two games are indistinguishable if normal form MLWE is hard.

Lemma 4. *The LIT Π_{LIT} has non-invertability (Definition 13) in the random oracle model if normal form $\text{sMLWE}_{q,\mathcal{R},k,\chi}$ is hard.*

Proof. Let \mathcal{A} be an adversary against the invertability of the LIT. We construct an adversary \mathcal{B} against normal form search-MLWE from it. \mathcal{B} simulates \mathcal{A} by using batching m samples from his MLWE oracle into a public key pk . By the definition of the MLWE oracle, there is some secret \mathbf{s} that was used to generate these samples. When \mathcal{A} asks for a tag on a previously unqueried message μ , \mathcal{B} uses its MLWE oracle to get a batch of m samples (\mathbf{A}, \mathbf{b}) , defines $\mathcal{RO}(\mu) := \mathbf{A}$ and answers with \mathbf{b} . If \mathcal{A} asks for a tag on a previously queried μ , \mathcal{B} answers with the \mathbf{b} it generated before. When \mathcal{A} outputs some $\text{sk}' = (\mathbf{s}', \mathbf{e}')$, \mathcal{B} returns \mathbf{s}' to its challenger. Due to Lemma 1 we know that the secret \mathbf{s} behind the tags is unique, therefore we know $\mathbf{s} = \mathbf{s}'$ if \mathcal{A} wins and thus \mathbf{s}' is a valid solution for normal form search-MLWE. \square

Lemma 5. *The LIT Π_{LIT} is linkable (Definition 11) in the random oracle model.*

Proof. The adversary can only win, if $f(\text{sk}_0) = f(\text{sk}_1)$. This means, that $\mathbf{s}_0^t \mathbf{A} + \mathbf{e}_0^t = \mathbf{s}_1^t \mathbf{A} + \mathbf{e}_1^t$, where $\text{sk}_i = (\mathbf{s}_i, \mathbf{e}_i)$. Due to Lemma 1 we know that the short MLWE secrets are unique, meaning $\mathbf{s}_0 = \mathbf{s}_1$. Therefore we know that $\mathbf{t}_0 - \mathbf{t}_1 = \mathbf{s}_0^t \mathbf{A}_\mu + \mathbf{e}_0^t - \mathbf{s}_1^t \mathbf{A}_\mu - \mathbf{e}_1^t = \mathbf{e}_0^t - \mathbf{e}_1^t$ for some $\mathbf{e}'_i, i \in \{0, 1\}$ with $\|\mathbf{e}'_i\|_\infty \leq \beta$. Thus we have $\|\mathbf{t}_0 - \mathbf{t}_1\|_\infty \leq 2\beta$ which is why the Link algorithm always outputs 1, meaning an adversary cannot win the linking game. \square

Lemma 6. *The LIT Π_{LIT} is unforgeable (Definition 12) in the random oracle model if normal form $\text{sMLWE}_{q,\mathcal{R},k,\chi}$ is hard.*

Proof. Let \mathcal{A} be an adversary against the unforgeability of the LIT and let Q be the number of oracle queries of \mathcal{A} . Construct an adversary \mathcal{B} against normal form search-MLWE. \mathcal{B} uses the first m samples of its oracle as the pk and gives that to \mathcal{A} . Then, on tag-query μ , \mathcal{B} asks its oracle for m samples batched as (\mathbf{A}, \mathbf{b}) , programs the random oracle as $\mathcal{RO}(\mu) := \mathbf{A}$ and returns \mathbf{b} . This way, there is a consistent \mathbf{s} behind the pk and tags \mathcal{A} sees, although \mathcal{B} does not know it. Then, \mathcal{A} outputs some sk^*, μ and t^* . If the tag is valid and links to some tag t , \mathcal{B} outputs \mathbf{s}^* , where $\text{sk}^* = (\mathbf{s}^*, \cdot)$. Now, due to Lemma 1 and the choice of β we know that the probability that $\mathbf{s} \neq \mathbf{s}^*$ is negligible. Therefore, if \mathcal{A} finds a forgery, \mathcal{B} outputs a solution for normal form search-MWLE with overwhelming probability. \square

Other Constructions It is also possible to base similar constructions on the security of Learning With Errors, Learning With Rounding or Module Learning With Rounding [BPR12]. For the latter two, this simplifies all algorithms, as we no longer have to consider the error or how to sample it and can, for example, simply check for equality of tags when linking them.

4 Reputation System

The first step to our reputation system is a syntax model. We base our model on [BJK15], but add some changes. In our model, we define four different (types of) parties: the group manager, the opener, an issuer and a user. In contrast to [BJK15], we identify a user by some user public key upk , which he can generate himself and for which he possesses some user secret key usk . Then, he can join the reputation system by interacting with the group manager, who knows some group manager key pair $(\text{gmsk}, \text{gmpk})$, with which he generates a registration token ρ to give to the user. Note that the joining of new users is dynamic and the number of users is not limited. Then, the user interacts with the issuer. The latter is identified by some issuer public key ipk , for which he knows some issuer secret isk . The issuer gives the user some rating token τ enabling the user to rate the issuer. Note that in contrast to [BJK15], the party to be rated is the issuer and not a product of an issuer. The user rates the issuer by using his usk , ρ and τ , where the latter was issued by the issuer to be rated, to create a signature for the rating. Anybody can verify the signature to check that the rating is valid, while not being able to see which user created the signature. Should the user rate the same issuer twice, anybody can use the linking algorithm to detect that two ratings were created by the same user. The last party is the opener, which in contrast to [BJK15] is a separate party from the group manager. The opener knows some opener secret key osk for some opener public key opk . In the case that a user misbehaves, the opener open a signature to break anonymity of the user, i.e. identify the user who created the signature. Note that the group manager and opener generate their secret keys separately, which is why our model offers a stronger security model than [BJK15]. We now give the formal definition of a reputation system.

Definition 15. *A reputation system consists of the following algorithms:*

- $\text{Setup}(1^n)$: *The ppt algorithm outputs some public parameters pp . We implicitly assume that all algorithms have pp as additional input.*
- $\text{KeyGen}_M(1^n)$: *The ppt algorithm outputs a pair of group manager secret and public key $(\text{gmsk}, \text{gmpk})$.*
- $\text{KeyGen}_O(1^n)$: *The ppt algorithm outputs a pair of opening secret and public key (osk, opk) .*
- $\text{KeyGen}_I(1^n)$: *The ppt algorithm outputs a pair of issuer secret and public key (isk, ipk) .*
- $\text{KeyGen}_U(1^n)$: *The ppt algorithm outputs a pair of user secret and public key (usk, upk) .*

- $\text{Join}(\text{gmpk}, \text{usk}), \text{Register}(\text{gmsk}, \text{upk})$: At the end of their interaction of these interactive ppt algorithms, Join outputs a registration token ρ .
- $\text{Request}(\text{gmpk}, \text{ipk}, \text{usk}, \rho), \text{Issue}(\text{gmpk}, \text{isk}, \text{upk})$: At the end of the interaction of these interactive ppt algorithms, Request outputs a rating token τ .
- $\text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}, \text{usk}, \rho, \tau, \text{rtng})$: The ppt algorithm outputs a signature σ .
- $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma)$. The ppt algorithm outputs a bit b .
- $\text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma)$: The ppt algorithm outputs some upk .
- $\text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}', \sigma'), (\text{rtng}'', \sigma''))$: The ppt algorithm outputs a bit b .

Definition 16. A reputation system is correct if for all security parameters n , all $\text{pp} \in [\text{Setup}(1^n)]$, all $(\text{gmsk}, \text{gmpk}) \in [\text{KeyGen}_M(1^n)]$, all $(\text{osk}, \text{opk}) \in [\text{KeyGen}_O(1^n)]$, all $(\text{isk}, \text{ipk}) \in [\text{KeyGen}_I(1^n)]$, all $(\text{usk}, \text{upk}_i) \in [\text{KeyGen}_U(1^n)]$, all $\rho \in [\text{Join}(\text{gmpk}, \text{usk}_i) \leftrightarrow \text{Register}(\text{gmsk}, \text{upk})]$, all $\tau \in [\text{Request}(\text{gmpk}, \text{ipk}, \text{usk}_i, \rho_i) \leftrightarrow \text{Issue}(\text{gmpk}, \text{isk}, \text{upk})]$, all ratings rtng , all $\sigma \in [\text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}, \text{usk}_i, \rho, \tau, \text{rtng})]$, all ratings rtng' , all $\sigma' \in [\text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}, \text{usk}, \rho, \tau, \text{rtng}')] it holds that$

- $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma_i) = 1$
- $\text{Open}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma_i) = \text{upk}_i$
- $\text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}, \sigma), (\text{rtng}', \sigma')) = 1$.

4.1 Security Model

Next we define the security model of a reputation system. We consider five different notions called anonymity, non-frameability, traceability, public-linkability and joining security. These notions are inspired by the model of [BJK15], except for non-frameability, which replaces strong-exculpability, and joining security, which is new since we split the group manager and opener into two parties.

In our security games, we model corruption differently than [BJK15] and [EKS18]. Instead of giving the adversary oracles to corrupt parties, we assume that every participant is corrupted, except for the minimal set that is needed so that the security experiment is not trivially solvable. We note that this model of corruption does not change the security level, it simply makes it easier to argue in proofs. Then, since we differentiate between the group manager and issuers, we can corrupt only one of them if needed. More importantly, this allows us model full corruption, meaning the adversary can choose the public keys *freely* for corrupted parties, where in [EKS18] the adversary also has to output a valid secret key for the public key he outputs. We also assume that the adversary carries a state in between its calls. Note that we do not consider concurrency.

Before we define the security experiments, we define some oracles that an adversary \mathcal{A} may have access to.

$\text{Rg}(\text{gmsk}, \text{upk})$: Run $\mathcal{A} \leftrightarrow \text{Register}(\text{gmsk}, \text{upk})$. Add upk to \mathcal{U} .

$\text{Req}(\text{gmpk}, \text{ipk}, u)$: If the input was queried before, output \perp . Else, run

$\tau_{u, \text{ipk}} \leftarrow \text{Request}(\text{gmpk}, \text{ipk}, \text{usk}_u, \rho_u) \leftrightarrow \mathcal{A}$ and store the rating token $\tau_{u, \text{ipk}}$.

SigO(gmpk, opk, ipk, u , rtng): If $\tau_{u, \text{ipk}}$ is undefined or the input was queried before, output \perp . Else, output $\sigma_{u, \text{ipk}} \leftarrow \text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}, \text{usk}_u, \tau_{u, \text{ipk}}, \text{rtng})$. Add $(\text{ipk}, \text{rtng}, \sigma_{u, \text{ipk}})$ to \mathcal{Q} .

Iss(gmpk, isk, upk): Add upk to \mathcal{I} . Run $\mathcal{A} \leftrightarrow \text{Issue}(\text{gmpk}, \text{isk}, \text{upk})$.

Note that in the security games, some of these parameters are fixed and cannot be chosen by the adversary. For the Rg oracle, for example, we fix gmsk , but leave upk open and thus write $\text{Rg}(\text{gmsk}, \cdot)$ in the JoinSecurity game.

The first security requirement for users is that they stay anonymous. In the anonymity experiment, we have two honest users that we try to protect. Except for these two users and the opener, we assume that every other party is corrupted, i.e. controlled by the adversary. In contrast to the notion of full-anonymity of group signature we only have selfless anonymity, meaning it is possible for a user to identify his own signatures. Thus, the usks of the honest users should stay hidden to the adversary.

$\text{Anon}_{\Pi, \mathcal{A}, b}(n)$
1 : $\text{pp} \leftarrow \text{Setup}(1^n)$
2 : $(\text{osk}, \text{opk}) \leftarrow \text{KeyGen}_O(1^n)$
3 : $\text{gmpk} \leftarrow \mathcal{A}(\text{opk})$
4 : For $u \in \{0, 1\}$
5 : $(\text{usk}_u, \text{upk}_u) \leftarrow \text{KeyGen}_U(1^n)$
6 : $\rho_u \leftarrow \text{Join}(\text{gmpk}, \text{usk}_u) \leftrightarrow \mathcal{A}(\text{upk}_u)$
7 : If $\rho_u = \perp$, return 0.
8 : $\text{ipk}^* \leftarrow \mathcal{A}^{\text{Req}(\text{gmpk}, \cdot, \cdot), \text{SigO}(\text{gmpk}, \text{opk}, \cdot, \cdot, \cdot), \text{Open}(\text{gmpk}, \text{osk}, \cdot, \cdot, \cdot)}$
9 : $\tau_u \leftarrow \text{Request}(\text{gmpk}, \text{ipk}^*, \text{usk}_u, \rho_u) \leftrightarrow \mathcal{A}$ for $u \in \{0, 1\}$
10 : If $\tau_u = \perp$ for any $u \in \{0, 1\}$, return 0.
11 : $\text{rtng} \leftarrow \mathcal{A}^{\text{Req}(\text{gmpk}, \cdot, \cdot), \text{SigO}(\text{gmpk}, \text{opk}, \cdot, \cdot, \cdot), \text{Open}(\text{gmpk}, \text{osk}, \cdot, \cdot, \cdot)}$
12 : $\sigma \leftarrow \text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}^*, \text{usk}_b, \rho_b, \tau_b, \text{rtng})$
13 : $b' \leftarrow \mathcal{A}^{\text{Req}(\text{gmpk}, \cdot, \cdot), \text{SigO}(\text{gmpk}, \text{opk}, \cdot, \cdot, \cdot), \text{Open}(\text{gmpk}, \text{isk}, \cdot, \cdot, \cdot)}(\sigma)$
14 : If there was a query to Open with $(\text{gmpk}, \text{osk}, \cdot, \cdot, \sigma)$ as argument, return 0.
15 : If there was a query to SigO with $(\text{gmpk}, \text{opk}, \text{ipk}^*, \cdot, \cdot)$ as argument, return 0.
16 : Return b' .

Definition 17. A reputation system Π is anonymous, if there exists a negligible function, such that for all ppt adversaries \mathcal{A} it holds that

$$\text{Adv}_{\Pi, \mathcal{A}}^{\text{anon}}(n) := |\Pr[\text{Anon}_{\Pi, \mathcal{A}, 0}(n) = 1] - \Pr[\text{Anon}_{\Pi, \mathcal{A}, 1}(n) = 1]| \leq \text{negl}(n).$$

Another security requirement for users is non-frameability. This expresses that any adversary can neither create a signature that opens to an honest user nor create a signature that links to one of an honest user, where the latter security requirement was added by [EKS18]. In the security experiment, we have one user

to be protected. In contrast to [EKS18], here and in all further security games, we require that the keys of the opener are generated honestly. This is due to the fact that we do not include a Judge algorithm as [EKS18] do.

NFrame $_{\Pi, \mathcal{A}}(n)$	
1 :	$\text{pp} \leftarrow \text{Setup}(1^n)$
2 :	$\mathcal{Q} = \emptyset$
3 :	$(\text{osk}, \text{opk}) \leftarrow \text{KeyGen}_O(1^n)$
4 :	$\text{gmpk} \leftarrow \mathcal{A}(\text{osk})$
5 :	$(\text{usk}_0, \text{upk}_0) \leftarrow \text{KeyGen}_U(1^n)$
6 :	$\rho_0 \leftarrow \text{Join}(\text{gmpk}, \text{usk}_0) \leftrightarrow \mathcal{A}(\text{upk}_0)$
7 :	$(\text{ipk}, \text{rtng}, \sigma) \leftarrow \mathcal{A}^{\text{Req}(\text{gmpk}, \cdot, 0), \text{SigO}(\text{gmpk}, \text{opk}, \cdot, 0, \cdot)}()$
8 :	$\text{upk} \leftarrow \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma)$
9 :	If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 0$, return 0
10 :	If $(\text{ipk}, \text{rtng}, \cdot) \in \mathcal{Q}$, return 0
11 :	If $\text{upk} = \text{upk}_0$, return 1
12 :	If $\exists (\text{ipk}, \text{rtng}', \sigma') \in \mathcal{Q} : \text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}, \sigma), (\text{rtng}', \sigma')) = 1$, return 1

Definition 18. A reputation system Π has non-frameability, if there exists a negligible function negl , such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{NFrame}_{\Pi, \mathcal{A}}(n) = 1] \leq \text{negl}(n).$$

An issuer requires traceability from the reputation system, which means that it is not possible to create a signature that does not open to some user or that opens to a user that was not given a rating token by an honest issuer. Here, we create one honest issuer that we want to protect.

Trace $_{\Pi, \mathcal{A}}(n)$	
1 :	$\text{pp} \leftarrow \text{Setup}(1^n)$
2 :	$\mathcal{I} = \emptyset$
3 :	$(\text{osk}, \text{opk}) \leftarrow \text{KeyGen}_O(1^n)$
4 :	$(\text{isk}, \text{ipk}) \leftarrow \text{KeyGen}_I(1^n)$
5 :	$\text{gmpk} \leftarrow \mathcal{A}(\text{osk}, \text{ipk})$
6 :	$(\sigma, \text{rtng}) \leftarrow \mathcal{A}^{\text{Iss}(\text{gmpk}, \text{isk}, \cdot)}()$
7 :	If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 0$, return 0
8 :	$\text{upk} \leftarrow \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma)$
9 :	If $\text{upk} = \perp \vee \text{upk} \notin \mathcal{I}$, return 1

Definition 19. A reputation system Π has traceability, if there exists a negligible function negl , such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{Trace}_{\Pi, \mathcal{A}}(n) = 1] \leq \text{negl}(n).$$

A security guarantee for the whole system is public-linkability. This requires that the outputs of **Open** and **Link** are consistent to each other, meaning it is not possible for an adversary to create two ratings for the same issuer that open to the same user, but do not link.

$\text{PLinkable}_{\Pi, \mathcal{A}}(n)$
1 : $\text{pp} \leftarrow \text{Setup}(1^n)$
2 : $(\text{osk}, \text{opk}) \leftarrow \text{KeyGen}_O(1^n)$
3 : $(\text{gmpk}, \text{ipk}, (\sigma_j, \text{rtng}_j)_{j \in \{0,1\}}) \leftarrow \mathcal{A}(\text{osk})$
4 : If $\exists j \in \{0, 1\} : \text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}_j, \sigma_j) = 0$, return 0.
5 : If $\text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}_0, \sigma_0) \neq \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}_1, \sigma_1)$, return 0.
6 : If $\text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}_0, \sigma_0), (\text{rtng}_1, \sigma_1)) = 0$, return 1.

Definition 20. A reputation system Π has public-linkability, if there exists a negligible function negl , such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{PLinkable}_{\Pi, \mathcal{A}}(n) = 1] \leq \text{negl}(n).$$

The group manager also has a security requirement. He wants that every user who wants to join the system must register with him and does not circumvent him. Else, issuers can invent non-existent users to rate themselves or their products.

$\text{JoinSecurity}_{\Pi, \mathcal{A}}(n)$
1 : $\text{pp} \leftarrow \text{Setup}(1^n)$
2 : $\mathcal{U} = \emptyset$
3 : $(\text{gmsk}, \text{gmpk}) \leftarrow \text{KeyGen}_M(1^n)$
4 : $(\text{osk}, \text{opk}) \leftarrow \text{KeyGen}_O(1^n)$
5 : $(\text{ipk}, \text{rtng}, \sigma) \leftarrow \mathcal{A}^{\text{Rg}(\text{gmsk}, \cdot)}(\text{gmpk}, \text{osk})$
6 : If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 0$, return 0.
7 : $\text{upk} \leftarrow \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma)$
8 : If $\text{upk} \notin \mathcal{U}$, output 1.

Definition 21. A reputation system Π has join-security, if there exists a negligible function negl , such that for all ppt adversaries \mathcal{A} it holds that

$$\Pr[\text{JoinSecurity}_{\Pi, \mathcal{A}}(n) = 1] \leq \text{negl}(n).$$

4.2 Generic Construction

We construct a reputation system from a signature scheme, an encryption scheme, a LIT, and a NIZK.

Construction 22. Let $\Sigma = (\text{KeyGen}_\Sigma, \text{Sign}_\Sigma, \text{Vrfy}_\Sigma)$ be a signature scheme. Let $\Pi_{\text{Enc}} = (\text{KeyGen}_{\text{Enc}}, \text{Enc}, \text{Dec})$ be an encryption scheme. Let $\Pi_{\text{LIT}} = (\text{KeyGen}_{\text{LIT}}, \text{Tag}, \text{Vrfy}_{\text{LIT}}, \text{Link}_{\text{LIT}}, f)$ be a LIT scheme. Let Π_{NIZK} be a non-interactive proof system for the relation listed in the “NIZK” expression below.

- $\text{Setup}(1^n)$: Run $\text{pp} \leftarrow \Pi_{\text{NIZK}}.\text{Setup}(1^n)$.
- $\text{KeyGen}_M(1^n)$: Run $(\text{gmsk}, \text{gmpk}) \leftarrow \text{KeyGen}_\Sigma(1^n)$.
- $\text{KeyGen}_O(1^n)$: Run $(\text{sk}_{\text{Enc}}, \text{pk}_{\text{Enc}}) \leftarrow \text{KeyGen}_{\text{Enc}}(1^n)$ and $(\text{sk}'_{\text{Enc}}, \text{pk}'_{\text{Enc}}) \leftarrow \text{KeyGen}_{\text{Enc}}(1^n)$. Set $(\text{osk}, \text{opk}) = (\text{sk}_{\text{Enc}}, (\text{pk}_{\text{Enc}}, \text{pk}'_{\text{Enc}}))$ and forget sk'_{Enc} .
- $\text{KeyGen}_I(1^n)$: Run $(\text{isk}, \text{ipk}) \leftarrow \text{KeyGen}_\Sigma(1^n)$.
- $\text{KeyGen}_U(1^n)$: Choose $\text{usk} \leftarrow \text{KeyGen}_{\text{LIT}}(1^n)$ and compute $\text{upk} = f(\text{usk})$.
- $\text{Join}(\text{gmpk}, \text{usk}), \text{Register}(\text{gmsk}, \text{upk})$: The group manager signs $\rho \leftarrow \text{Sign}_\Sigma(\text{gmsk}, \text{upk})$ and sends ρ to the user. If $\text{Vrfy}_\Sigma(\text{gmpk}, \text{upk}, \rho)$, the user outputs it.
- $\text{Request}(\text{gmpk}, \text{ipk}, \text{usk}, \rho), \text{Issue}(\text{gmpk}, \text{isk}, \text{upk})$: The issuer signs $\tau \leftarrow \text{Sign}_\Sigma(\text{isk}, \text{upk})$ and sends τ to the user. If $\text{Vrfy}_\Sigma(\text{ipk}, \text{upk}, \tau)$, the user outputs it.
- $\text{Sign}(\text{gmpk}, \text{opk}, \text{ipk}, \text{usk}, \rho, \tau, \text{rtng})$: Compute $c = \text{Enc}(\text{pk}_{\text{Enc}}, \text{upk}; r)$. Compute $c' = \text{Enc}(\text{pk}'_{\text{Enc}}, \text{usk}; r')$. Compute $l = \text{Tag}(\text{usk}, \text{ipk}; r_t)$. Output $\sigma = (c, c', l, \pi)$, where

$$\begin{aligned} \pi = \text{NIZK}\{ & \text{gmpk}, \text{opk}, \text{ipk}, \text{pk}_{\text{Enc}}, \text{pk}'_{\text{Enc}}, c, c', l; \\ & \text{upk}, \text{usk}, \rho, \tau, r, r' ; \text{upk} = f(\text{usk}) \wedge \\ & \text{Vrfy}_\Sigma(\text{gmpk}, \text{upk}, \rho) = 1 \wedge \\ & \text{Vrfy}_\Sigma(\text{ipk}, \text{upk}, \tau) = 1 \wedge \\ & c = \text{Enc}(\text{pk}_{\text{Enc}}, \text{upk}; r) \wedge \\ & c' = \text{Enc}(\text{pk}'_{\text{Enc}}, \text{usk}; r') \wedge \\ & \text{Vrfy}_{\text{LIT}}(\text{usk}, \text{ipk}, l) = 1\}(\text{rtng}) \end{aligned}$$

- $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma)$: Verify π for the corresponding statement.
- $\text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma)$: Verify π for the corresponding statement. If π is valid, output $\text{upk} = \text{Dec}(\text{osk}, c)$.
- $\text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}', \sigma'), (\text{rtng}'', \sigma''))$: Verify π', π'' for the corresponding statements. If π', π'' are valid, output $\text{Link}_{\text{LIT}}(\text{ipk}, l', l'')$.

The correctness of the construction follows directly from the correctness of its building blocks.

4.3 Security of the Generic Construction

The encryption of usk with pk'_{Enc} in a rating is not necessary for functionality, but a crucial component for the security proof. This is similar to the Naor-Yung paradigm to get CCA security of an encryption scheme from CPA security. Without the encryption of usk we would have to assume online simulation-extractability (we use the terminology found in [Don+22])— that it is hard for

an adversary to create a valid proof from which an extractor cannot extract, even if the adversary sees simulated proofs for possibly wrong statements not in the language, and the extractor needs to be able to extract during protocol execution, not just at the end – instead of simulation soundness from the NIZK. This is a significantly stronger assumption on the proof system, so we choose to encrypt the usk and to require simulation-soundness.

Theorem 1. *If Π_{Enc} is CPA secure (Definition 35), the LIT has indistinguishable tags (Definition 10) and Π_{NIZK} has zero-knowledgeness and simulation-soundness (Definitions 4 and 6), the reputation system is anonymous (Definition 17).*

Note that by our modelling of NIZKs, this theorem and the other security theorems of the generic construction hold in the random oracle model. However, as stated in Section 2.2, they can be adapted to hold in the standard model.

Proof. We prove this by a series of games. An overview can be found in Table 1.

	π	Challenge	Query	Tag	Opening
Game ₀	\mathcal{P}	$c \equiv \text{upk}_0$ $c' \equiv \text{usk}_0$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₀	Dec(sk _{Enc} , c)
Game ₁	\mathcal{S}	$c \equiv \text{upk}_0$ $c' \equiv \text{usk}_0$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₀	Dec(sk _{Enc} , c)
Game ₂	\mathcal{S}	$c \equiv \text{upk}_0$ $c' \equiv 1^{ \text{usk}_0 }$	$c \equiv \text{upk}_u$ $c' \equiv 1^{ \text{usk}_u }$	usk ₀	Dec(sk _{Enc} , c)
Game ₃	\mathcal{S}	$c \equiv \text{upk}_0$ $c' \equiv 1^{ \text{usk}_0 }$	$c \equiv \text{upk}_u$ $c' \equiv 1^{ \text{usk}_u }$	usk ₁	Dec(sk _{Enc} , c)
Game ₄	\mathcal{S}	$c \equiv \text{upk}_0$ $c' \equiv \text{usk}_1$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₁	Dec(sk _{Enc} , c)
Game ₅	\mathcal{S}	$c \equiv \text{upk}_0$ $c' \equiv \text{usk}_1$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₁	$f(\text{Dec}(\text{sk}'_{\text{Enc}}, c'))$
Game ₆	\mathcal{S}	$c \equiv \text{upk}_1$ $c' \equiv \text{usk}_1$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₁	$f(\text{Dec}(\text{sk}'_{\text{Enc}}, c'))$
Game ₇	\mathcal{S}	$c \equiv \text{upk}_1$ $c' \equiv \text{usk}_1$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₁	Dec(sk _{Enc} , c)
Game ₈	\mathcal{P}	$c \equiv \text{upk}_1$ $c' \equiv \text{usk}_1$	$c \equiv \text{upk}_u$ $c' \equiv \text{usk}_u$	usk ₁	Dec(sk _{Enc} , c)

Table 1. An overview of the sequence of games for the anonymity proof. The column π states whether proofs are done honestly (\mathcal{P}) or simulated (\mathcal{S}). The columns *Challenge* and *Query* state what messages are encrypted in the ciphertexts c, c' during the generation of the challenge or the signature query answer. *Tag* states which secret is used to generate a tag. *Opening* states how opening is done.

Define $\epsilon_{\mathcal{D},a,b}(n)$ to be the advantage of some ppt \mathcal{D} distinguishing Game_a(n) from Game_b(n). Let Game₀ be the Anon₀ game. Define Game₁ to be the same

game as Game_0 , except that the challenger uses the simulator \mathcal{S} of Π_{NIZK} (Definition 4) to generate all proofs, including the challenge. We immediately see that an adversary cannot distinguish between these games, as the difference of the distribution of the proofs is negligible due to the zero-knowledge property of the proof system. Thus, we have that for all ppt distinguishers \mathcal{D} , there exists a ppt \mathcal{A}_0 such that

$$\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_0}^{\text{ZK}}(n) = \epsilon_{\mathcal{D}, 0, 1}(n).$$

Define Game_2 to be the same game as Game_1 except that c' in the signature queries is generated as $c' \leftarrow \text{Enc}(\text{pk}'_{\text{Enc}}, 1^{|\text{usk}_u|})$, i.e. we encrypt a string of ones instead of usk_u . Furthermore, c' in the challenge is generated as $c' \leftarrow \text{Enc}(\text{pk}'_{\text{Enc}}, 1^{|\text{usk}_0|})$, i.e. we encrypt a string of ones instead of usk_0 . This is indistinguishable by the CPA security of the encryption scheme. By a standard hybrid argument we can construct a ppt \mathcal{A} against the CPA security of Π_{Enc} from a distinguisher \mathcal{D} such that

$$\text{Adv}_{\Pi_{\text{Enc}}, \mathcal{A}_1}^{\text{CPA}}(n) = \frac{1}{Q+1} \epsilon_{\mathcal{D}, 1, 2}(n).$$

Define Game_3 to be the same game as Game_2 except that tags l in the signature queries and the challenge are computed as $l \leftarrow \text{Tag}(\text{usk}_1, \text{ipk}; r_t)$, i.e. we use usk_1 instead of usk_0 . This is indistinguishable by the tag-indistinguishability of Π_{LIT} (Definition 10). Let \mathcal{D} be distinguisher distinguishing Game_2 and Game_3 . Construct an adversary \mathcal{A}_2 against the tag-indistinguishability of the LIT.

- On input $(\text{pk}_0, \text{pk}_1)$ set up the reputation system as in Game_2 , except for setting $\text{upk}_0 := \text{pk}_0, \text{upk}_1 := \text{pk}_1$.
- Simulate \mathcal{D} .
- Whenever \mathcal{D} asks for a signature, query the oracle for a tag l and use that to create the signature. Do the same for the challenge.
- If \mathcal{D} returns a bit b , return b .

We can easily see that if \mathcal{A}_2 's challenger is in experiment $b = 0$, the view of \mathcal{D} is the same as in Game_2 , else the view is the same as in Game_3 . Thus, we have the following.

$$\text{Adv}_{\Pi_{\text{LIT}}, \mathcal{A}_2}^{\text{LITAnon}}(n) = \epsilon_{\mathcal{D}, 2, 3}(n)$$

Define Game_4 to be the same game as Game_3 except that c' in the signature queries is generated as $c' \leftarrow \text{Enc}(\text{pk}'_{\text{Enc}}, \text{usk}_u; r')$, i.e. we again encrypt usk_u instead of $1^{|\text{usk}_u|}$, and c' in the challenge is generated as $c' \leftarrow \text{Enc}(\text{pk}'_{\text{Enc}}, \text{upk}_1; r')$, i.e. we encrypt usk_1 instead of $1^{|\text{usk}_0|}$. By the CPA security of the encryption scheme we immediately have the following for an adversary \mathcal{A}_3 that simulates a distinguisher \mathcal{D} as in Game_3 , by a similar argument as above:

$$\text{Adv}_{\Pi_{\text{Enc}}, \mathcal{A}_3}^{\text{CPA}}(n) = \frac{1}{Q+1} \epsilon_{\mathcal{D}, 3, 4}(n)$$

Define Game_5 to be the same game as Game_4 except that opening is done by remembering sk'_{Enc} during key generation, decrypting c' to some usk and outputting $f(\text{usk})$ instead of outputting the decryption of c . An adversary can only distinguish between these games if he can submit an opening query $(\text{ipk}, \text{rtng}, \sigma)$ with $\sigma = (c, c', l, \pi)$ such that π is valid but $\text{Dec}(\text{sk}_{\text{Enc}}, c) \neq f(\text{Dec}(\text{sk}'_{\text{Enc}}, c'))$ and such that σ is not an answer he received from the signature oracle. Call the event that an adversary outputs such a query Fake . However, if an adversary could submit such a query, this would break the simulation-soundness of Π_{NIZK} (Definition 6). To show this, from a distinguisher \mathcal{D} between Game_4 and Game_5 we construct an adversary \mathcal{A}_4 against the simulation-soundness of Π_{NIZK} .

- On input some pp_{NIZK} , set up Game_4 while remembering $\text{sk}_{\text{Enc}}, \text{sk}'_{\text{Enc}}$ and setting $\text{pp} = \text{pp}_{\text{NIZK}}$.
- Simulate \mathcal{D} . To simulate proofs, \mathcal{A} uses its simulator oracle.
- Whenever \mathcal{D} makes an opening query on $(\text{ipk}, \text{rtng}, \sigma)$, answer as in Game_4 . Additionally, if $\sigma = (c, c', l, \pi)$ is not an answer from a previous signing query and $\text{upk} \neq \text{upk}'$, where $\text{upk} \leftarrow \text{Dec}(\text{sk}_{\text{Enc}}, c)$ and $\text{upk}' \leftarrow f(\text{Dec}(\text{sk}'_{\text{Enc}}, c'))$, stop and output the statement from σ together with π .
- If \mathcal{D} stops, output a failure symbol \perp .

If \mathcal{A}_4 finds a query such that $\text{upk} \neq \text{upk}'$ and the σ is not from a signature query, we know that, while π is valid and is not a response from the simulator oracle, the statement is not in the language. Therefore, this σ together with the corresponding statement is a proof that breaks the simulation-soundness. Thus, we have that

$$\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_4}^{SS}(n) = \Pr[\text{Fake}] \geq \epsilon_{\mathcal{D}, 4, 5}(n).$$

Define Game_6 to be the same game as Game_5 except that c in the challenge σ is generated as $c \leftarrow \text{Enc}(\text{pk}_{\text{Enc}}, \text{upk}_1; r)$, i.e. we encrypt upk_1 instead of upk_0 . This is again indistinguishable by the CPA security of the encryption scheme, thus for a distinguisher \mathcal{D} and an adversary \mathcal{A}_5 constructed similarly to above we have

$$\text{Adv}_{\Pi_{\text{Enc}}, \mathcal{A}_5}^{CPA}(n) = \epsilon_{\mathcal{D}, 5, 6}(n)$$

Define Game_7 to be the same game as Game_6 except that opening is done honestly again, i.e. by decrypting c . Again, from a distinguisher \mathcal{D} we can construct an adversary \mathcal{A}_6 against the simulation-soundness of Π_{NIZK} similar to above and we get

$$\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_6}^{SS}(n) \geq \epsilon_{\mathcal{D}, 6, 7}(n)$$

Define Game_8 to be the same game as Game_7 except that the proofs are generated honestly again, thus we have that Game_8 is the same as Anon_1 . This is again indistinguishable due to the zero-knowledge property of Π_{NIZK} . Thus, we have that for all distinguishers \mathcal{D} , there exists an \mathcal{A}_7 such that

$$\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_7}^{ZK}(n) = \epsilon_{\mathcal{D}, 7, 8}(n).$$

Therefore, in total for any ppt distinguishers \mathcal{D}_i for $i \in \{0, \dots, 7\}$ we have that

$$\begin{aligned} \text{Adv}_{\Pi, \mathcal{A}}^{\text{anon}}(n) &\leq \sum_{i=0}^7 \epsilon_{\mathcal{D}_i, i, i+1}(n) \\ &\leq 2\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_0}^{\text{ZK}}(n) + \text{Adv}_{\Pi_{\text{LIT}}, \mathcal{A}_2}^{\text{LITAnon}}(n) \\ &\quad + (2Q + 3)\text{Adv}_{\Pi_{\text{Enc}}, \mathcal{A}_1}^{\text{CPA}}(n) \\ &\quad + 2\text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{A}_4, \mathcal{S}}^{\text{SS}}(n) = 1] \end{aligned}$$

□

Theorem 2. *If Π_{LIT} is non-invertible and unforgeable (Definitions 12 and 13) and Π_{NIZK} has zero-knowledgeness and simulation-soundness (Definition 4 and 6), the reputation system has non-frameability (Definition 18).*

Proof. When an adversary against non-frameability wins, we have that the forgery either opens to the honest user or it links to a rating of the honest user. From these cases, we construct an adversary that targets either the non-invertibility or the unforgeability of Π_{LIT} . We also need to analyze the probability of some failure event, for which we use the simulation-soundness of Π_{NIZK} .

Let \mathcal{A} be an adversary against the non-frameability (Definition 18) of the reputation scheme that does at most q queries to the signing oracle. Let **Fail** be the event that in the non-frameability game the statement of the proof contained in the forgery of \mathcal{A} is wrong, i.e. it is not in the language of the relation. Construct an adversary \mathcal{B} against the non-invertibility (Definition 13) of Π_{LIT} as follows:

- On input pk , simulate $\text{NFrame}_{\Pi, \mathcal{A}}(n)$, except for setting $\text{upk}_0 = \text{pk}$ and remembering sk'_{Enc} .
- When \mathcal{A} queries the request oracle, use the simulator of Π_{NIZK} (cf. Definition 4) to answer the query. If it queries the signature oracle, use the tag oracle to generate a tag, generate c, c' honestly, then use the simulator of Π_{NIZK} to generate the proof.
- Eventually, \mathcal{A} outputs some forgery $(\text{ipk}, \text{rtng}, \sigma)$ with $\sigma = (c, c', l, \pi)$. If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 1$ and $u := \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma) = \text{upk}_0$, then $\text{usk} \leftarrow \text{Dec}(\text{sk}'_{\text{Enc}}, c')$.
- Output usk .

We can easily see that the view of \mathcal{A} is perfectly simulated, except for negligible error from simulating the proofs. If \mathcal{A} could distinguish the views, we could immediately construct \mathcal{C} that breaks the zero-knowledgeness of Π_{NIZK} . Then, we know that if \mathcal{A} manages to output a valid signature that opens to upk_0 , and **Fail** does not happen, it holds that $\text{pk} = f(\text{usk})$. Thus, we have the following.

$$\Pr[\text{Invert}_{\Pi_{\text{LIT}}, \mathcal{B}} = 1] \geq \Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 \wedge u = \text{upk}_0 \wedge \neg \text{Fail}] + \text{Adv}_{\Pi_{\text{NIZK}}, \mathcal{C}}^{\text{ZK}}(n)$$

We also construct a \mathcal{C} against the unforgeability of Π_{LIT} (Definition 12).

- On input pk , simulate $\text{NFrame}_{\Pi, \mathcal{A}}(n)$ except for setting $\text{upk}_0 = \text{pk}$. Also save sk'_{Enc} .
- When \mathcal{A} queries the request oracle, use Π_{NIZK} simulator to answer the query. If \mathcal{A} queries the signature oracle, use the tag oracle to generate a tag, then use the simulator of Π_{NIZK} to answer the query with the corresponding statement.
- \mathcal{A} outputs $(\text{ipk}, \text{rtng}, \sigma)$ with $\sigma = (c, c', \pi, l)$. If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 1$ and $u := \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma) \neq \text{upk}_0$ and $\exists (\text{ipk}, \text{rtng}, \hat{\sigma}) \in Q$ with $\hat{\sigma} = (\hat{c}, \hat{c}', \hat{\pi}, \hat{l})$ such that $\text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}, \sigma), (\text{rtng}, \hat{\sigma})) = 1$ and $\text{rtng} \neq \text{rtng}$, then decrypt $\text{usk} \leftarrow \text{Dec}(\text{sk}'_{\text{Enc}}, c')$ and output $(\text{usk}, \text{ipk}, l)$.

Again, we can easily see that the view of \mathcal{A} is perfectly simulated. If \mathcal{A} outputs a forgery $(\text{ipk}, \text{rtng}, \sigma)$ such that

$$\begin{aligned} & \text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 1 \\ & \text{and } u := \text{Open}(\text{gmpk}, \text{osk}, \text{ipk}, \text{rtng}, \sigma) \neq \text{upk}_0 \\ & \text{and } \exists (\text{ipk}, \text{rtng}) \in Q : \text{Link}(\text{gmpk}, \text{opk}, \text{ipk}, (\text{rtng}, \sigma), (\text{rtng}, \hat{\sigma})) = 1 \\ & \text{and Fail does not happen,} \end{aligned}$$

we know that by definition we have $\text{Vrfy}_{\text{LIT}}(\text{usk}, \text{ipk}, l) = 1$ and $\text{Link}_{\text{LIT}}(\text{ipk}, l, \hat{l}) = 1$. Therefore we have the following.

$$\Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 | \neg \text{Fail} \wedge u \neq \text{upk}_0] = \Pr[\text{Forge}_{\Pi_{\text{LIT}}, C}^{\text{LIT}} = 1]$$

Lastly, we want to analyze the probability $\Pr[\text{Fail}]$. For this, we construct an adversary \mathcal{D} against the simulation-soundness of Π_{NIZK} (Definition 6):

- On input crs , simulate $\text{NFrame}_{\Pi, \mathcal{A}}(n)$ except for using the provided crs .
- Simulate \mathcal{A} . Whenever \mathcal{A} makes an oracle query such that the answer would contain a NIZK, use the simulator oracle to generate the proof.
- \mathcal{A} outputs some forgery $(\text{ipk}, \text{rtng}, \sigma)$. If $\text{Vrfy}(\text{gmpk}, \text{opk}, \text{ipk}, \text{rtng}, \sigma) = 1$, return σ and the corresponding statement.

We can easily see that \mathcal{A} is perfectly simulated and that if Fail happens, \mathcal{D} wins. Therefore we can bound the non-frameability advantage of \mathcal{A} .

$$\begin{aligned} \Pr[\text{NFrame}_{\Pi, \mathcal{A}}] & \leq \Pr[\text{NFrame}_{\Pi, \mathcal{A}} \wedge \neg \text{Fail}] + \Pr[\text{Fail}] \\ & = \Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 \wedge \neg \text{Fail} \wedge u = \text{upk}_0] \\ & \quad + \Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 \wedge \neg \text{Fail} \wedge u \neq \text{upk}_0] + \Pr[\text{Fail}] \\ & \leq \Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 | \neg \text{Fail} \wedge u = \text{upk}_0] \\ & \quad + \Pr[\text{NFrame}_{\Pi, \mathcal{A}} = 1 | \neg \text{Fail} \wedge u \neq \text{upk}_0] + \Pr[\text{Fail}] \\ & = \Pr[\text{Invert}_{\Pi_{\text{LIT}}, \mathcal{B}} = 1] + \Pr[\text{Forge}_{\Pi_{\text{LIT}}, C}^{\text{LIT}} = 1] \\ & \quad + \Pr[\text{SimSound}_{\Pi_{\text{NIZK}}, \mathcal{D}, \mathcal{S}} = 1] \end{aligned}$$

□

Theorem 3. *If Σ is EUF-CMA (Definition 37) and Π_{NIZK} is straight-line extractable (Definition 7), the reputation system is traceable (Definition 19).*

Proof. Let $\mathcal{E}_0, \mathcal{E}_1$ be the extractor for Π_{NIZK} (cf. Definition 7). Let \mathcal{A} be a ppt adversary against traceability. First, we define $\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n)$ to work like $\text{Trace}_{\Pi_{\text{NIZK}}, \mathcal{A}}(n)$, except that the public parameters pp are generated by the extractor, i.e. $(\text{pp}, td) \leftarrow \mathcal{E}_0(1^n)$. From the guarantees of the extractor (Definition 7) and a straight-forward reduction, we get that $|\Pr[\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1] - \Pr[\text{Trace}_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1]| \leq \text{negl}_0(n)$ for some negligible function negl_0 .

We construct an adversary \mathcal{B} against the unforgeability of Σ . $\mathcal{B}^{\text{Sign}(\text{sk}, \cdot)}(\text{pk})$ runs $\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n)$, except that it sets $\text{ipk} = \text{pk}$ and whenever \mathcal{A} makes a $\text{lss}(\text{gmpk}, \text{isk}, \text{upk})$ query, \mathcal{B} answers by querying its own oracle $\text{Sign}(\text{sk}, \text{upk})$ for the signature. Eventually, \mathcal{A} outputs (σ, rtng) , where $\sigma = (c, c', l, \pi)$. \mathcal{B} runs $\mathcal{E}_1(td, x, \text{rtng}, \pi)$ (where x is set appropriately to the proven statement) to receive a witness $w = (\text{upk}, \text{usk}, \rho, \tau, r, r')$. \mathcal{B} outputs (upk, τ) as a candidate forgery.

Let $\text{fail}_{\mathcal{E}}$ be the event that $\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1$, but \mathcal{E}_1 outputs an invalid witness (i.e. $(x, w) \notin \mathfrak{R}$). With a straight-forward reduction to straight-line extractability, we can show that $\Pr[\text{fail}_{\mathcal{E}}] \leq \text{negl}_1(n)$ for some negligible function negl_1 . If $\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1$ and $\neg \text{fail}_{\mathcal{E}}$, \mathcal{B} outputs a valid forgery. This is because the Trace' winning condition “ $\text{upk} \notin \mathcal{I}$ ” (together with $(x, w) \in \mathfrak{R}$ and correctness of the encryption scheme guarantees that \mathcal{B} has not queried its signing oracle for upk with overwhelming probability. Hence there exists a negligible function negl_2 such that

$$\begin{aligned} & \text{Adv}_{\Sigma, \mathcal{A}}^{\text{EUF-CMA}}(n) \\ & \geq \Pr[\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1 \wedge \neg \text{fail}_{\mathcal{E}}] - \text{negl}_2(n) \\ & = \Pr[\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1] - \Pr[\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1 \wedge \text{fail}_{\mathcal{E}}] - \text{negl}_2(n) \\ & \geq \Pr[\text{Trace}'_{\Pi_{\text{NIZK}}, \mathcal{A}}(n) = 1] - \text{negl}_1(n) - \text{negl}_2(n) \end{aligned}$$

□

Theorem 4. *If Σ is EUF-CMA (Definition 37) and Π_{NIZK} is straight-line extractable (Definition 7), the reputation system has joining security (Definition 21).*

The proof is analogous to the proof of Theorem 3.

Theorem 5. *If Π_{LIT} is linkable (Definition 11) and Π_{NIZK} has soundness, the reputation system is publicly linkable (Definition 20).*

Proof. Let \mathcal{A} be an adversary against the public linkability of the reputation system. We construct an adversary \mathcal{B} against the linkability of Π_{LIT} from it:

- Simulate $\text{PLinkable}_{\Pi, \mathcal{A}}(n)$.
- \mathcal{A} outputs some gmpk and ipk and forgery-rating pairs $(\sigma_j, \text{rtng}_j)_{j \in \{0,1\}}$, where $\sigma_j = (c_j, c'_j, l_j, \pi_j)$.

- If both σ_j are valid signatures in the simulated public-linkability game and do not link, decrypt c'_0, c'_1 to get $\text{usk}_0, \text{usk}_1$ and output $(\text{usk}_0, \text{usk}_1, \text{ipk}, l_0, l_1)$.

If \mathcal{A} outputs gmpk, ipk with two forgeries σ_0, σ_1 that are valid for these keys and the opk , due to soundness of Π_{NIZK} we have that $\text{Vrfy}_{\text{LIT}}(\text{usk}_j, \text{ipk}, l_j) = 1$ for $j \in \{0, 1\}$. Then, again due to the soundness of Π_{NIZK} , we have that $f(\text{usk}_0) = f(\text{usk}_1)$. Call **Sound** the event that \mathcal{A} outputs such tags or such ciphertexts that the above conditions do not hold. Then, we can construct an adversary \mathcal{C} against the soundness of Π_{NIZK} , by simply outputting the proof that \mathcal{A} outputs. Thus, we know that $\Pr[\text{Sound}] \leq \text{Adv}_{\Pi, \mathcal{A}}^{\text{Snd}}(n)$. If the σ_j do not link, it follows that $(\text{usk}_0, \text{usk}_1, \text{ipk}, l_0, l_1)$ is a tuple of two valid tags for the same message created with $\text{usk}_0, \text{usk}_1$ respectively, which do not link. Therefore, we have that

$$\Pr[\text{Linkable}_{\Pi, \text{LIT}, \mathcal{C}}^{\text{LIT}}(n) = 1] = \Pr[\text{PLinkable}_{\Pi, \mathcal{A}}(n) = 1] + \text{Adv}_{\Pi, \mathcal{A}}^{\text{Snd}}(n).$$

□

The Role of Straight-Line Extraction For the proof of traceability (Theorem 3) and joining security (Theorem 4), we require Π_{NIZK} to be straight-line extractable, i.e. the proof system must not rely on rewinding for extraction (which, for example, Fiat-Shamir-based proofs usually do). In our security proofs for Theorems 3 and 4, the reduction algorithm has access to a signature oracle. Similarly to what was noted in [FN16], this represents an issue for an extractor: when rewinding the reduction algorithm \mathcal{B} , the extractor needs to answer \mathcal{B} 's signing oracle queries. However, in standard definitions, the extractor does not have access to the signing oracle. Even if we grant access, the extractor querying the signing oracle may actually cause an extracted forgery to become invalid. This happens in case a signature on the forgery message is being requested by \mathcal{B} during rewinding. There are potential ways to circumvent this issue for specific proof systems, but standard definitions of (rewinding-based) soundness are incompatible with signing oracle access in security proofs. Straight-line extraction does not suffer from this issue, as the extractor can be used without rewinding.

One can always implement straight-line extractable proofs by encrypting the witness for some honestly generated publicly known public key and proving, with a *sound* zero-knowledge proof, that the encrypted witness is valid. Note that in our security proofs for Theorems 3 and 4, the only value we need to extract from the proof is the membership certificate τ or ρ (upk is also used, but can be computed by decrypting c). For this reason, when implementing straight-line extractability, it suffices to additionally encrypt τ and ρ , there is no need to encrypt the *full* witness of the rating NIZK.

Alternatively, one can use a NIZK that is inherently straight-line extractable (e.g., using Fischlin's transform [Fis05a] or Katsumata's transform [Kat21]). In these cases, it also suffices to extract only a part of the witness, namely ρ, τ . In practice, one can arguably even use a standard Fiat-Shamir-based construction, for which one cannot prove straight-line extractability (cf. [BNW17]). However, to the best of our knowledge, there is no attack against Fiat-Shamir in practice that targets schemes using it in place of a straight-line extractable proof.

5 A Reputation System from Module Lattices

We now want to instantiate the generic construction with building blocks based on module lattices. Since we only used generally common concepts, we are relatively free in choosing which actual building blocks we want to use. However, we need to make sure they fit together, especially with the NIZK, meaning that we can prove the statements defined by our other building blocks. The NIZK of our choice is, as mentioned previously in Corollary 1, the proof system of [LNP22b] transformed into a straight-line extractable NIZK by Katsumata’s transform [Kat21]. With it, we can create proofs for the relation \mathfrak{R}^R (cf. Definition 8), so we have to argue that we can express our statements to prove via this relation.

For the LIT, we choose the scheme presented in Construction 14. To instantiate Construction 22 with it, we need to prove possession of a secret usk and secret upk , such that $f(\text{usk}) = \text{upk}$. Since this boils down to showing possession of an MLWE secret for a secret \mathbf{b} , this can be realized as shown in Table 2. Due to our choice of the encryption scheme, we use the bit-decomposition of the upk . Thus, we also need to prove that one knows $\text{upk}, \text{BitD}(\text{upk})$ such that $\text{upk} = \mathbf{G} \cdot \text{BitD}(\text{upk})$ and $\text{BitD}(\text{upk})$ is a bit vector, which is also possible. Since this works similar to showing possession of an MLWE secret for *public* \mathbf{b} as shown in [LNP22b], we roughly estimate the proof for the former to be of size 30KB.

variable	description	instantiation
ϕ	# of equations to prove	1
ϕ_{eval}	# of evaluations with const. coeff. zero	0
v_e	# of exact norm proofs	2
v_d	# of non-exact norm proofs	0
k_{bin}	length of the binary vector to prove	$m_U \log q$
\mathbf{s}_1	committed message in the Ajtai part	$(\mathbf{t}^t, \mathbf{e}^t, \text{BitD}(\text{upk})^t)^t$
\mathbf{m}	committed message in the BDLOP part	\emptyset (no message)
f_1	equation to prove	$\mathbf{A}' \mathbf{s}_1 = 0$
\mathbf{D}_1	public matrix for proving $\ \mathbf{E}_1 \mathbf{s} - \mathbf{u}_1\ _\infty \leq \beta_1^{(e)}$	$[\mathbf{I} \ \mathbf{0} \ \mathbf{0}]$
\mathbf{u}_1	public vector for proving $\ \mathbf{E}_1 \mathbf{s} - \mathbf{u}_1\ _\infty \leq \beta_1^{(e)}$	$\mathbf{0}$
$\beta_1^{(d)}$	upper bound on $\ \mathbf{E}_1 \mathbf{s} - \mathbf{u}_1\ _\infty \leq \beta_1^{(e)}$	β
\mathbf{D}_2	public matrix for proving $\ \mathbf{E}_2 \mathbf{s} - \mathbf{u}_2\ _\infty \leq \beta_2^{(e)}$	$[\mathbf{0} \ \mathbf{I} \ \mathbf{0}]$
\mathbf{u}_2	public vector for proving $\ \mathbf{E}_2 \mathbf{s} - \mathbf{u}_2\ _\infty \leq \beta_2^{(e)}$	$\mathbf{0}$
$\beta_2^{(d)}$	upper bound on $\ \mathbf{E}_2 \mathbf{s} - \mathbf{u}_2\ _\infty \leq \beta_2^{(e)}$	β
\mathbf{E}_{bin}	matrix for proving binary	$[\mathbf{0} \ \mathbf{0} \ \mathbf{I}]$
\mathbf{v}_{bin}	vector for proving binary	0

Table 2. Proving possession of a usk for secret upk . Define $\mathbf{A}' = [\mathbf{A}'_T \mid \mathbf{I} \mid -\mathbf{G}]$.

For the encryption scheme, we use the MLWE variant of the primal Regev encryption scheme that is presented in [LNP22b] as their verifiable encryption

scheme. There they also show that one can create a proof showing the validity of a ciphertext, which we need in our generic construction. However, their scheme has a message space of $\{0, 1\}^n$, while we want to encrypt a $\text{upk} \in \mathcal{R}_q^m$. Thus, we instead encrypt the bit-decomposition $\text{BitD}(\text{upk})$ of the upk in multiple ciphertexts. Based on the parameters in [LNP22b], we estimate the proof size showing the ciphertext to be valid to be 4762KB. We expect other lattice-based encryption schemes such as Kyber [Bos+18], Saber [DAn+18] and NTRU [HPS98] to also work for our generic construction, as [LNP22b] claim they work in their proof system.

To instantiate the signature scheme, we need it to be compatible with our NIZK. Signature schemes that use the random oracle, such as Fiat-Shamir-with-aborts signature scheme [Lyu09] or hash-then-sign signatures [GPV08; MP12], are not suitable. Instead, we use signature schemes in the standard model, such as [DM14], and we focus on signatures that are either specifically designed for use in combination with proofs of knowledge, such as [JRS23], or are very efficient [Boo+23]. An overview comparing the schemes can be found in Table 3.

Scheme	State	Assumption	Proof Size
[DM14] and our adaption	stateless	RSIS	–
[JRS23][JRS22, Appendix H]	stateless	MSIS	–
[JRS23] and our adaptations	stateful	MSIS	163584 KB
[Boo+23]	stateless	Int-NTRU-ISIS _f	59392 KB

Table 3. Overview over different candidate signature schemes to instantiate the reputation system with. For the definition of the Int-NTRU-ISIS_f problem, see [Boo+23]. Proof size refers to size of a NIZK in kilobytes in the framework of [LNP22b] proving possession of a secret message-signature pair for 128-bit security. These are conservative estimates for message space $\{0, 1\}^{nm \cdot \log q}$.

The signature scheme of [DM14] is shown to be secure for non-adaptive queries, to be converted to adaptive security via chameleon hash. However, one can show that using a technique similar to [LSS14] using the Rényi divergence, that the scheme has adaptive security without the chameleon hash. For details, see Appendix B, which also describes how to prove possession of a secret message-signature pair in the framework of [LNP22b]. However, the signature scheme has reduction loss dependent on the success probability of the adversary, which leads to large parameters. The stateless signature scheme of [JRS23; JRS22] is designed in such a way that the verification equation works well with relations that can be proven by lattice-based proofs of knowledge. In particular, [JRS23] already show that one can show possession of a message-signature pair of their scheme in the framework of [LNP22b]. This signature scheme suffers from the same reduction loss drawback as [DM14] though, since they use the same proof technique of prefix-guessing of a tag.

In [Boo+23] they introduce a credential system based on novel security assumptions that are related to ISIS. Their credential system can also be seen as

a (blind) signature, of which one proves possession, thus we can instantiate our signature scheme and the proof with it. The most efficient credential system they design is based on the so-called Int-NTRU-ISIS_f problem and achieves a proof size of 29KB (under some heuristics) for a message space of $\{0, 1\}^{16}$. If we use the construction of [Boo+23] and the other aforementioned building blocks, we arrive at a total proof size for the instantiation of the generic construction of $30\text{KB} + 4762\text{KB} + 59392\text{KB} = 64184\text{KB}$. Note that this is a very rough estimate and we expect careful analysis to yield a much better proof size.

Stateful reputation system Parallel to the stateless variant, [JRS23] also construct a stateful ℓ -time signature scheme based on MSIS. They show the size of a proof showing possession of a secret message-signature pair to be 693KB for a message in $\{0, 1\}^{128}$, also using the proof system of [LNP22b]. It is possible to use stateful signatures in our generic construction, by changing the model of the reputation system such that the group manager and issuers are stateful, i.e. the Join and Issue algorithms get some state as input. We also allow only a fixed number ℓ of users to join the system. The correctness and security model have to be changed accordingly, which is straight-forward. Both are not unreasonable assumptions to make in practice, as group managers have to keep track how many members there are in the system anyways and issuers have to store information about their sales, making both inherently stateful. Furthermore, for large enough ℓ , e.g. 2^{40} , this amount of users will likely not be reached in practice. The security proofs for the stateful reputation system basically work as for the stateless reputation system, except for using stateful and ℓ -time signatures instead of stateless ones.

Instead of the stateful signatures of [JRS23], one can use an adaption (cf. Appendix C.1), which is a slightly simplified version of the former getting rid of the commitment in the signing process. There is a second adaption, which can be more efficient than the signature of [JRS23] depending on the degree of the ring, since its security relies on RLWE, NTRU and RSIS instead of MSIS. Details can be found in Appendix C.2.

5.1 Instantiation with Pairing-Based Cryptography

To instantiate the generic construction based on pairing-based cryptography, we use the following constructions for the building blocks:

- The linking indistinguishable tags are $t = \mathcal{RO}(\text{ipk})^{\text{usk}}$ with $f(\text{usk}) = g^{\text{usk}}$. Two tags t_0, t_1 link if $t_0 = t_1$.
- The signature scheme to sign the user’s public key g^{usk} is a simplified version of the structure-preserving signature [Gro15], namely $\sigma = (\tilde{R}, S, T) = (\tilde{g}^r, (y \cdot g^w)^{1/r}, (y^w \cdot M)^{1/r})$ (as in [Bob+21]), where signatures are valid iff they are of that form (can be checked using the pairing).
- The encryption scheme for the user’s public key is ElGamal, the encryption scheme for $\text{usk} \in \mathbb{Z}_p$ is bitwise raised ElGamal.
- The NIZK is a simple Schnorr-like protocol made straight-line extractable with Fischlin’s transform [Fis05b; KS22].

We leave the details of the instantiation to the reader.

Acknowledgement We would like to thank the anonymous reviewers for their helpful comments and constructive feedback.

References

- [AFK22] Thomas Attema, Serge Fehr, and Michael Kloos. “Fiat-Shamir Transformation of Multi-round Interactive Proofs”. In: *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part I*. Ed. by Eike Kiltz and Vinod Vaikuntanathan. Vol. 13747. Lecture Notes in Computer Science. Springer, 2022, pp. 113–142. DOI: [10.1007/978-3-031-22318-1_5](https://doi.org/10.1007/978-3-031-22318-1_5).
- [BE17] Rachid El Bansarkhani and Ali El Kaafarani. “Direct Anonymous Attestation from Lattices”. In: *IACR Cryptol. ePrint Arch.* (2017), p. 1022. URL: <http://eprint.iacr.org/2017/1022>.
- [BEJ18] Johannes Blömer, Fabian Eidens, and Jakob Juhnke. “Practical, Anonymous, and Publicly Linkable Universally-Composable Reputation Systems”. In: *Topics in Cryptology - CT-RSA 2018 - The Cryptographers’ Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*. Ed. by Nigel P. Smart. Vol. 10808. Lecture Notes in Computer Science. Springer, 2018, pp. 470–490. DOI: [10.1007/978-3-319-76953-0_25](https://doi.org/10.1007/978-3-319-76953-0_25).
- [Ben+19] Eli Ben-Sasson et al. “Aurora: Transparent Succinct Arguments for R1CS”. 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 I*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. Lecture Notes in Computer Science. Springer, 2019, pp. 103–128. DOI: [10.1007/978-3-030-17653-2_4](https://doi.org/10.1007/978-3-030-17653-2_4).
- [BJK15] Johannes Blömer, Jakob Juhnke, and Christina Kolb. “Anonymous and Publicly Linkable Reputation Systems”. In: *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*. Ed. by Rainer Böhme and Tatsuaki Okamoto. Vol. 8975. Lecture Notes in Computer Science. Springer, 2015, pp. 478–488. DOI: [10.1007/978-3-662-47854-7_29](https://doi.org/10.1007/978-3-662-47854-7_29).
- [BNW17] David Bernhard, Ngoc Khanh Nguyen, and Bogdan Warinschi. “Adaptive Proofs Have Straightline Extractors (in the Random Oracle Model)”. In: *Applied Cryptography and Network Security - 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings*. Ed. by Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi. Vol. 10355. Lecture Notes in Computer Science. Springer, 2017, pp. 336–353. DOI: [10.1007/978-3-319-61204-1_17](https://doi.org/10.1007/978-3-319-61204-1_17).

- [Bob+21] Jan Bobolz et al. “Issuer-Hiding Attribute-Based Credentials”. In: *Cryptography and Network Security - 20th International Conference, CANS 2021, Vienna, Austria, December 13-15, 2021, Proceedings*. Ed. by Mauro Conti, Marc Stevens, and Stephan Krenn. Vol. 13099. Lecture Notes in Computer Science. Springer, 2021, pp. 158–178. DOI: [10.1007/978-3-030-92548-2_9](https://doi.org/10.1007/978-3-030-92548-2_9).
- [Boo+23] Jonathan Bootle et al. “A Framework for Practical Anonymous Credentials from Lattices”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part II*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14082. Lecture Notes in Computer Science. Springer, 2023, pp. 384–417. DOI: [10.1007/978-3-031-38545-2_13](https://doi.org/10.1007/978-3-031-38545-2_13).
- [Bos+18] Joppe W. Bos et al. “CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM”. In: *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*. IEEE, 2018, pp. 353–367. DOI: [10.1109/EuroSP.2018.00032](https://doi.org/10.1109/EuroSP.2018.00032).
- [Bos+20] Cecilia Boschini et al. “Efficient Post-quantum SNARKs for RSIS and RLWE and Their Applications to Privacy”. In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*. Ed. by Jintai Ding and Jean-Pierre Tillich. Vol. 12100. Lecture Notes in Computer Science. Springer, 2020, pp. 247–267. DOI: [10.1007/978-3-030-44223-1_14](https://doi.org/10.1007/978-3-030-44223-1_14).
- [Bou+23] Katharina Boudgoust et al. “On the Hardness of Module Learning with Errors with Short Distributions”. In: *J. Cryptol.* 36.1 (2023), p. 1. DOI: [10.1007/s00145-022-09441-3](https://doi.org/10.1007/s00145-022-09441-3).
- [Boy10] Xavier Boyen. “Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More”. In: *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*. Ed. by Phong Q. Nguyen and David Pointcheval. Vol. 6056. Lecture Notes in Computer Science. Springer, 2010, pp. 499–517. DOI: [10.1007/978-3-642-13013-7_29](https://doi.org/10.1007/978-3-642-13013-7_29).
- [BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. “Pseudorandom Functions and Lattices”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 719–737. DOI: [10.1007/978-3-642-29011-4_42](https://doi.org/10.1007/978-3-642-29011-4_42).
- [BSS10] John Bethencourt, Elaine Shi, and Dawn Song. “Signatures of Reputation”. In: *Financial Cryptography and Data Security, 14th International Conference, FC 2010, Tenerife, Canary Islands, Spain, January 25-28, 2010, Revised Selected Papers*. Ed. by Radu Sion.

- Vol. 6052. Lecture Notes in Computer Science. Springer, 2010, pp. 400–407. DOI: [10.1007/978-3-642-14577-3_35](https://doi.org/10.1007/978-3-642-14577-3_35).
- [Che+19] Liqun Chen et al. “A Framework for Efficient Lattice-Based DAA”. In: *Proceedings of the 1st ACM Workshop on Workshop on Cyber-Security Arms Race, CYSARM@CCS 2019, London, UK, November 15, 2019*. Ed. by Liqun Chen et al. ACM, 2019, pp. 23–34. DOI: [10.1145/3338511.3357349](https://doi.org/10.1145/3338511.3357349).
- [CL06] Melissa Chase and Anna Lysyanskaya. “On Signatures of Knowledge”. In: *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*. Ed. by Cynthia Dwork. Vol. 4117. Lecture Notes in Computer Science. Springer, 2006, pp. 78–96. DOI: [10.1007/11818175_5](https://doi.org/10.1007/11818175_5).
- [CS97] Jan Camenisch and Markus Stadler. “Efficient Group Signature Schemes for Large Groups (Extended Abstract)”. In: *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*. Ed. by Burton S. Kaliski Jr. Vol. 1294. Lecture Notes in Computer Science. Springer, 1997, pp. 410–424. DOI: [10.1007/BFb0052252](https://doi.org/10.1007/BFb0052252).
- [DAn+18] Jan-Pieter D’Anvers et al. “Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM”. In: *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*. Ed. by Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi. Vol. 10831. Lecture Notes in Computer Science. Springer, 2018, pp. 282–305. DOI: [10.1007/978-3-319-89339-6_16](https://doi.org/10.1007/978-3-319-89339-6_16).
- [DLP14] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. “Efficient Identity-Based Encryption over NTRU Lattices”. In: *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*. Ed. by Palash Sarkar and Tetsu Iwata. Vol. 8874. Lecture Notes in Computer Science. Springer, 2014, pp. 22–41. DOI: [10.1007/978-3-662-45608-8_2](https://doi.org/10.1007/978-3-662-45608-8_2).
- [DM14] Léo Ducas and Daniele Micciancio. “Improved Short Lattice Signatures in the Standard Model”. In: *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*. Ed. by Juan A. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Springer, 2014, pp. 335–352. DOI: [10.1007/978-3-662-44371-2_19](https://doi.org/10.1007/978-3-662-44371-2_19).
- [Don+22] Jelle Don et al. “Online-Extractability in the Quantum Random-Oracle Model”. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applica-*

- tions of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 677–706. DOI: [10.1007/978-3-031-07082-2_24](https://doi.org/10.1007/978-3-031-07082-2_24).
- [DRS04] Yevgeniy Dodis, Leonid Reyzin, and Adam D. Smith. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”. In: *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*. Ed. by Christian Cachin and Jan Camenisch. Vol. 3027. Lecture Notes in Computer Science. Springer, 2004, pp. 523–540. DOI: [10.1007/978-3-540-24676-3_31](https://doi.org/10.1007/978-3-540-24676-3_31).
- [EKS18] Ali El Kaafarani, Shuichi Katsumata, and Ravital Solomon. “Anonymous Reputation Systems Achieving Full Dynamicity from Lattices”. In: *Financial Cryptography and Data Security - 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 - March 2, 2018, Revised Selected Papers*. Ed. by Sarah Meiklejohn and Kazue Sako. Vol. 10957. Lecture Notes in Computer Science. Springer, 2018, pp. 388–406. DOI: [10.1007/978-3-662-58387-6_21](https://doi.org/10.1007/978-3-662-58387-6_21).
- [Fis05a] Marc Fischlin. “Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors”. In: *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*. Ed. by Victor Shoup. Vol. 3621. Lecture Notes in Computer Science. Springer, 2005, pp. 152–168. DOI: [10.1007/11535218_10](https://doi.org/10.1007/11535218_10).
- [Fis05b] Marc Fischlin. “Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors”. In: *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*. Ed. by Victor Shoup. Vol. 3621. Lecture Notes in Computer Science. Springer, 2005, pp. 152–168. DOI: [10.1007/11535218_10](https://doi.org/10.1007/11535218_10).
- [FN16] Dario Fiore and Anca Nitulescu. “On the (In)Security of SNARKs in the Presence of Oracles”. In: *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*. Ed. by Martin Hirt and Adam D. Smith. Vol. 9985. Lecture Notes in Computer Science. 2016, pp. 108–138. DOI: [10.1007/978-3-662-53641-4_5](https://doi.org/10.1007/978-3-662-53641-4_5).
- [GG21] Stan Gurtler and Ian Goldberg. “SoK: Privacy-Preserving Reputation Systems”. In: *Proc. Priv. Enhancing Technol.* 2021.1 (2021), pp. 107–127. DOI: [10.2478/popets-2021-0007](https://doi.org/10.2478/popets-2021-0007).
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed.

- by Cynthia Dwork. ACM, 2008, pp. 197–206. DOI: [10.1145/1374376.1374407](https://doi.org/10.1145/1374376.1374407).
- [Gro15] Jens Groth. “Efficient Fully Structure-Preserving Signatures for Large Messages”. In: *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*. Ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9452. Lecture Notes in Computer Science. Springer, 2015, pp. 239–259. DOI: [10.1007/978-3-662-48797-6_11](https://doi.org/10.1007/978-3-662-48797-6_11).
- [HBB23] Omar Hasan, Lionel Brunie, and Elisa Bertino. “Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey”. In: *ACM Comput. Surv.* 55.2 (2023), 32:1–32:37. DOI: [10.1145/3490236](https://doi.org/10.1145/3490236).
- [HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. “NTRU: A Ring-Based Public Key Cryptosystem”. In: *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*. Ed. by Joe Buhler. Vol. 1423. Lecture Notes in Computer Science. Springer, 1998, pp. 267–288. DOI: [10.1007/BFb0054868](https://doi.org/10.1007/BFb0054868).
- [JRS22] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. *Lattice Signature with Efficient Protocols, Application to Anonymous Credentials*. Cryptology ePrint Archive, Paper 2022/509. 2022. URL: <https://eprint.iacr.org/2022/509>.
- [JRS23] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. “Lattice Signature with Efficient Protocols, Application to Anonymous Credentials”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part II*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14082. Lecture Notes in Computer Science. Springer, 2023, pp. 351–383. DOI: [10.1007/978-3-031-38545-2_12](https://doi.org/10.1007/978-3-031-38545-2_12).
- [Kat21] Shuichi Katsumata. “A New Simple Technique to Bootstrap Various Lattice Zero-Knowledge Proofs to QROM Secure NIZKs”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part II*. Ed. by Tal Malkin and Chris Peikert. Vol. 12826. Lecture Notes in Computer Science. Springer, 2021, pp. 580–610. DOI: [10.1007/978-3-030-84245-1_20](https://doi.org/10.1007/978-3-030-84245-1_20).
- [KS22] Yashvanth Kondi and Abhi Shelat. “Improved Straight-Line Extraction in the Random Oracle Model with Applications to Signature Aggregation”. In: *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part II*. Ed. by Shweta Agrawal and Dongdai

- Lin. Vol. 13792. Lecture Notes in Computer Science. Springer, 2022, pp. 279–309. DOI: [10.1007/978-3-031-22966-4_10](https://doi.org/10.1007/978-3-031-22966-4_10).
- [Lib+16] Benot Libert et al. “Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions”. In: *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10032. Lecture Notes in Computer Science. 2016, pp. 373–403. DOI: [10.1007/978-3-662-53890-6_13](https://doi.org/10.1007/978-3-662-53890-6_13).
- [Lin+17] San Ling et al. “Lattice-Based Group Signatures: Achieving Full Dynamism with Ease”. In: *Applied Cryptography and Network Security - 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings*. Ed. by Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi. Vol. 10355. Lecture Notes in Computer Science. Springer, 2017, pp. 293–312. DOI: [10.1007/978-3-319-61204-1_15](https://doi.org/10.1007/978-3-319-61204-1_15).
- [Lin+18] San Ling et al. “Constant-Size Group Signatures from Lattices”. In: *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II*. Ed. by Michel Abdalla and Ricardo Dahab. Vol. 10770. Lecture Notes in Computer Science. Springer, 2018, pp. 58–88. DOI: [10.1007/978-3-319-76581-5_3](https://doi.org/10.1007/978-3-319-76581-5_3).
- [LM19] Jia Liu and Mark Manulis. “pRate: Anonymous Star Rating with Rating Secrecy”. In: *Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*. Ed. by Robert H. Deng et al. Vol. 11464. Lecture Notes in Computer Science. Springer, 2019, pp. 550–570. DOI: [10.1007/978-3-030-21568-2_27](https://doi.org/10.1007/978-3-030-21568-2_27).
- [LNP22a] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 284. URL: <https://eprint.iacr.org/2022/284>.
- [LNP22b] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 71–101. DOI: [10.1007/978-3-031-15979-4_3](https://doi.org/10.1007/978-3-031-15979-4_3).
- [LPR13a] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. “A Toolkit for Ring-LWE Cryptography”. In: *IACR Cryptol. ePrint Arch.* (2013), p. 293. URL: <http://eprint.iacr.org/2013/293>.

- [LPR13b] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. “A Toolkit for Ring-LWE Cryptography”. In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 35–54. DOI: [10.1007/978-3-642-38348-9_3](https://doi.org/10.1007/978-3-642-38348-9_3).
- [LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. “GGHlite: More Efficient Multilinear Maps from Ideal Lattices”. In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 239–256. DOI: [10.1007/978-3-642-55220-5_14](https://doi.org/10.1007/978-3-642-55220-5_14).
- [Lyu+21] Vadim Lyubashevsky et al. “Shorter Lattice-Based Group Signatures via “Almost Free” Encryption and Other Optimizations”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. Lecture Notes in Computer Science. Springer, 2021, pp. 218–248. DOI: [10.1007/978-3-030-92068-5_8](https://doi.org/10.1007/978-3-030-92068-5_8).
- [Lyu09] Vadim Lyubashevsky. “Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures”. In: *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*. Ed. by Mitsuru Matsui. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 598–616. DOI: [10.1007/978-3-642-10366-7_35](https://doi.org/10.1007/978-3-642-10366-7_35).
- [MP12] Daniele Micciancio and Chris Peikert. “Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 700–718. DOI: [10.1007/978-3-642-29011-4_41](https://doi.org/10.1007/978-3-642-29011-4_41).
- [PLS18] Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler. “Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability”. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*. Ed. by David Lie et al. ACM, 2018, pp. 574–591. DOI: [10.1145/3243734.3243852](https://doi.org/10.1145/3243734.3243852).

A Uniqueness of (M)LWE Secrets

In Lemma 1, we claimed that for certain parameters, the secret of an MLWE sample is unique. We now want to prove this lemma.

Definition 23. Let \mathcal{R} be a finite ring. For $s \in \mathcal{R} \setminus \{0\}$ set

$$\mathcal{Z}_s := \{a \in \mathcal{R} \setminus \{0\} : a \cdot s = 0\}$$

and define

$$z_{\max} := \max\{|\mathcal{Z}_s| : s \in \mathcal{R} \setminus \{0\}\}.$$

Equivalently, $1 + z_{\max}$ is the maximal number of solutions in \mathcal{R} of an equation $x \cdot s = c$, for $s, c \in \mathcal{R}$.

Theorem 6. Let $m, k \in \mathbb{N}$, $D \subseteq \mathcal{R}^k$, $B \subseteq \mathcal{R}^m$. Then

$$\Pr [\exists (\mathbf{s}, \mathbf{e}) \in D \times B : \mathbf{s} \neq \mathbf{0} \wedge \mathbf{A} \cdot \mathbf{s} = \mathbf{e}; \mathbf{A} \leftarrow \mathcal{R}^{m \times k}] \leq \left(\frac{1 + z_{\max}}{|\mathcal{R}|} \right)^m \cdot |D| \cdot |B|.$$

Proof. Fix (\mathbf{s}, \mathbf{e}) , $\mathbf{e} = (e_1, \dots, e_m)$ as in the theorem. By definition of z_{\max}

$$\Pr [\mathbf{A}_i \cdot \mathbf{s} = e_i; \mathbf{A}_i \leftarrow \mathcal{R}^{1 \times k}] \leq \frac{1 + z_{\max}}{|\mathcal{R}|}.$$

Hence for fixed (\mathbf{s}, \mathbf{e})

$$\Pr [\mathbf{A} \cdot \mathbf{s} = \mathbf{e}; \mathbf{A} \leftarrow \mathcal{R}^{m \times k}] \leq \left(\frac{1 + z_{\max}}{|\mathcal{R}|} \right)^m.$$

By the union bound the theorem follows. \square

We now restate Lemma 1 with a bit more detail in order to prove it.

Lemma 7 (Short MLWE secrets are unique). Let $q \neq 2$ be a prime with $q = 3, 5 \pmod{8}$ (or $q = 1 \pmod{2n}$), $k > 0$, $n > 16$ be a power of 2, $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$. Let $B_\beta = \{e \in \mathcal{R}_q : \|e\|_\infty \leq \beta\}$. Let $\Delta \geq 0$ such that $2\beta + \Delta < q^{1/4}$. Then there exists some $d < n$ such that

$$\begin{aligned} \epsilon(n) := \Pr \left[\begin{array}{l} \exists (\mathbf{s}, \mathbf{s}', \mathbf{e}, \mathbf{e}') \in (B_\beta^k)^2 \times (B_\beta^m)^2 \\ \text{with } \mathbf{s} \neq \mathbf{s}' \wedge \|\mathbf{b}\|_\infty \leq \Delta \end{array} ; \mathbf{A} \leftarrow \mathcal{R}_q^{k \times m} \right. \\ \left. \mathbf{b}^t = (\mathbf{s} - \mathbf{s}')^t \mathbf{A} + (\mathbf{e} - \mathbf{e}')^t \right] \\ \leq \frac{(4\beta + 2\Delta + 1)^{n(m+k)}}{q^{md}}. \end{aligned}$$

Furthermore, there exists an m and a negligible function negl such that $\epsilon(n) \leq \text{negl}(n)$.

Proof. Assume there are some $\mathbf{s}, \mathbf{s}', \mathbf{e}, \mathbf{e}'$ with the conditions mentioned in the theorem. We define $\hat{\mathbf{s}} = \mathbf{s} - \mathbf{s}' \neq \mathbf{0}$ with $\|\hat{\mathbf{s}}\|_\infty \leq 2\beta$ and $\hat{\mathbf{e}} = \mathbf{e} - \mathbf{e}'$ with $\|\hat{\mathbf{e}}\|_\infty \leq 2\beta$. Then, since $\|\mathbf{A}\hat{\mathbf{s}} + \hat{\mathbf{e}}\|_\infty \leq \Delta$ holds, there exists some $\tilde{\mathbf{e}}$ with $\|\tilde{\mathbf{e}}\|_\infty \leq \Delta$ such that $\mathbf{A}\hat{\mathbf{s}} + \hat{\mathbf{e}} - \tilde{\mathbf{e}} = \mathbf{0}$. Thus we can use Theorem 6 to show that

$$\begin{aligned} \epsilon(n) &:= \Pr \left[\begin{array}{l} \exists (\mathbf{s}, \mathbf{s}', \mathbf{e}, \mathbf{e}') \in (B_\beta^k)^2 \times (B_\beta^m)^2 : \mathbf{A} \leftarrow \mathcal{R}_q^{k \times m} \\ \text{with } \mathbf{s} \neq \mathbf{s}' \wedge \|\mathbf{b}\|_\infty \leq \Delta : \mathbf{b}^t = (\mathbf{s} - \mathbf{s}')^t \mathbf{A} + (\mathbf{e} - \mathbf{e}')^t \end{array} \right] \\ &= \Pr [\exists (\hat{\mathbf{s}}, \hat{\mathbf{e}} - \tilde{\mathbf{e}}) \in B_{2\beta}^k \times B_{2\beta+\Delta}^m : \hat{\mathbf{s}} \neq \mathbf{0}, \mathbf{A}\hat{\mathbf{s}} + \hat{\mathbf{e}} - \tilde{\mathbf{e}} = \mathbf{0}; \mathbf{A} \leftarrow \mathcal{R}_q^{m \times k}] \\ &\leq \left(\frac{1 + z_{\max}}{|\mathcal{R}_q|} \right)^m |B_{2\beta}^k| \cdot |B_{2\beta+\Delta}^m| \end{aligned}$$

By the choice of q and n we know the polynomial $X^n + 1$ is irreducible over $\mathbb{Q}[X]$ and splits over $\mathbb{Z}_q[X]$ into factors of equal degree. Let this degree be d and, accordingly, the number of factors is n/d . Then it holds that

$$\mathcal{R}_q \cong \underbrace{\mathbb{F}_{q^d} \times \cdots \times \mathbb{F}_{q^d}}_{n/d},$$

where \mathbb{F}_{q^d} denotes the field with q^d elements. From this one sees that an element s maximizing $|\mathcal{Z}_s|$ is $(1, 0, \dots, 0)$ with

$$z_{\max} = |\mathcal{Z}_s| = (q^d)^{n/d-1} - 1 = q^{n-d} - 1.$$

This together with the fact that $|\mathcal{R}_q| = q^n$, results in

$$\epsilon(n) \leq \frac{(4\beta + 1)^{nk} \cdot (4\beta + 2\Delta + 1)^{nm}}{q^{md}} \leq \frac{(4\beta + 2\Delta + 1)^{n(m+k)}}{q^{md}}$$

If $n \geq 16$, $q = 3, 5 \pmod{8}$, then one can show that $d = n/2$. In this case, the probability above can be made negligibly small in n for q polynomially large in n and $\beta = q^\gamma$, $\gamma < 1/4$, even with $m = 1$. If $q = 1 \pmod{2n}$, then $d = 1$. In this case, for q polynomially in n , one has to pick $m > 1$ to make the probability above negligibly small in n . \square

One can also show that uniform secrets of the standard LWE problem are unique, if one chooses m correctly depending on n, q, β .

Corollary 2 (LWE secrets are unique). *Let q be a prime and $\beta > 0$. Set $B := \{\mathbf{e} \in \mathbb{Z}_q^m : \|\mathbf{e}\|_\infty \leq \beta\}$. Then*

$$\Pr [\exists (\mathbf{s}, \mathbf{e}) \in \mathbb{Z}_q^n \times B^m : \mathbf{s} \neq \mathbf{0} \wedge \mathbf{A} \cdot \mathbf{s} = \mathbf{e}; \mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n}] \leq \left(\frac{2\beta + 1}{q} \right)^m \cdot q^n.$$

B Adaptive Ducas-Micciancio Signatures

Before describing the signature scheme of [DM14], we need to define RSIS, Gaussian distributions and a notion of trapdoors.

Definition 24 (RSIS). Let $q > 2$ and $m, \beta > 0$. Let \mathcal{R} be a ring and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. The RSIS problem $\text{RSIS}_{q, \mathcal{R}, m, \beta}$ is given a uniform vector $\mathbf{a} \leftarrow \mathcal{R}_q^m$ to find a non-trivial vector $\mathbf{x} \in \mathcal{R}_q^m \setminus \{\mathbf{0}\}$ such that $\mathbf{a}^t \mathbf{x} = \mathbf{0}$ and $\|\mathbf{x}\| \leq \beta$.

Definition 25. Define the Gaussian function $\rho_{s, \mathbf{c}}(\mathbf{x}) = \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2)$. Define the discrete Gaussian distribution $D_{\Lambda + \mathbf{t}, s, \mathbf{c}}$ on a lattice coset $\Lambda + \mathbf{t}$ with center \mathbf{c} and parameter s as

$$D_{\Lambda + \mathbf{t}, s, \mathbf{c}}(\mathbf{x}) = \begin{cases} \frac{\rho_{s, \mathbf{c}}(\mathbf{x})}{\rho_{s, \mathbf{c}}(\Lambda + \mathbf{t})} & \text{if } \mathbf{x} \in \Lambda + \mathbf{t} \\ 0 & \text{else} \end{cases}$$

Define the discrete Gaussian distribution $D_{\mathcal{R}, s, c} = \theta^{-1}(D_{\theta(\mathcal{R}), s, \theta(c)})$ for a ring \mathcal{R} . If center $c = 0$, we omit it.

Definition 26 (G-trapdoor [MP12]). For a matrix $\mathbf{a}^t \in \mathcal{R}_q^{1 \times m}$, a G-trapdoor is a matrix $\mathbf{R} \in \mathcal{R}_q^{m \times \zeta}$ such that $\mathbf{a}^t \mathbf{R} = \mathbf{g}^t$ for a gadget matrix $\mathbf{g}^t \in \mathcal{R}_q^{1 \times \zeta}$.

We can generate such trapdoors with an algorithm called `GenTrap` and use them to sample preimages of some function for a given image with `PreSample`.

Theorem 7 ([MP12]). Let $\zeta \in \mathbb{N}$ and $m = \mathcal{O}(n \log q)$ large enough. Let $g = \lceil q^{1/\zeta} \rceil \in \mathcal{R}_q$ and $\mathbf{g}^t = [1 \mid g \mid \dots \mid g^{\zeta-1}]$. There exist ppt algorithms `GenTrap`, `PreSample` such that

- `GenTrap`($1^n, 1^m, q$) outputs $\mathbf{a}^t \in \mathcal{R}_q^{1 \times 2m}$ and $\mathbf{R} \in \mathcal{R}_q^{2m \times \zeta}$ such that $\mathbf{a}^t \mathbf{R} = \mathbf{g}^t$ and $\mathbf{R} \in \mathcal{R}_q^{2m \times \zeta}$ and the distribution of \mathbf{a}^t is statistically indistinguishable from uniform;
- `PreSample`($\mathbf{a}^t, \mathbf{R}, u, s$) on input a matrix $\mathbf{a}^t \in \mathcal{R}_q^{1 \times 2m}$, a matrix $\mathbf{R} \in \mathcal{R}_q^{2m \times \zeta}$ output by `GenTrap`, a syndrome $u \in \mathcal{R}_q$ and a standard deviation $s \geq \eta_e(\mathbb{Z}) \sqrt{g^2 + 1} \sqrt{\|\mathbf{R}\|^2}$ outputs \mathbf{v} that is statistically close to $D_{\mathcal{R}_q^{2m}, s}$ conditioned on $\mathbf{a}^t \mathbf{v} = u \pmod{q}$.

We now state the signature of [DM14] which can be used to instantiate our reputation system. We claim that it is (adaptively) EUF-CMA secure without any changes, while the original theorem by [DM14] only claims security for non-adaptive queries. [DM14] achieve adaptive security by a standard transformation of first hashing the message with a chameleon hash before signing it. However, one can adapt their security proof to directly show adaptive security by applying a technique similar to [LSS14] using the Rényi divergence.

The idea of the construction of [DM14] is that the public key contains some uniformly generated \mathbf{a}^t , while the secret key is a trapdoor for that \mathbf{a} . To sign a message \mathbf{m} , we first choose a random tag κ . Based on κ, \mathbf{a}^t and some public

matrices \mathbf{a}_i^t we define some \mathbf{a}_κ^t in such a way that we can adapt the trapdoor for \mathbf{a}^t to a trapdoor for \mathbf{a}_κ^t . We hash the message using some \mathbf{d}^t and add some public u to get $v = u + \mathbf{d}^t \mathbf{m}$. Then, we use `PreSample` to sample a short preimage σ of v under \mathbf{a}_κ^t . Signature verification is done by simply checking whether σ is indeed a short preimage of v and whether κ is in the tag space.

Construction 27. *Let the message space be $\mathcal{R}_2^{m_2}$. Let $g = \lceil q^{\frac{1}{\zeta}} \rceil$ and $\mathbf{g}^t = [1 \mid g \mid \dots \mid g^{\zeta-1}] \in \mathcal{R}_q^{1 \times \zeta}$. Let the tag space be $\mathcal{T} = \{0, 1\}^d$. Let $s = n^{3/2} \cdot \omega(\log n)^{3/2}$ such that $s^2 \geq (\sqrt{nm_1} + \sqrt{nm_2} + t)\sqrt{nm_2}$ for some t . Let $\beta = s\sqrt{n(m_1 + \zeta)}$.*

- `KeyGen`(1^n): Choose $(\mathbf{a}^t, \mathbf{R}) \leftarrow \text{GenTrap}(1^n, 1^{m_1}, q)$ such that $\mathbf{a}^t \in \mathcal{R}_q^{1 \times m_1}$, $\mathbf{R} \in \mathcal{R}_q^{m_1 \times \zeta}$ and $\mathbf{a}^t \mathbf{R} = \mathbf{g}^t$. Choose $\mathbf{a}_i^t \leftarrow \mathcal{R}_q^{1 \times m_1}$ for $i \in \{0, \dots, d\}$. Choose $\mathbf{d}^t \leftarrow \mathcal{R}_q^{1 \times m_2}$, $u \leftarrow \mathcal{R}_q$. Set $\text{pk} = (\mathbf{a}^t, \mathbf{a}_0^t, \dots, \mathbf{a}_d^t, \mathbf{d}^t, u)$ and $\text{sk} = \mathbf{R}$.
- `Sign`(sk, \mathbf{m}): Choose $\kappa \leftarrow \mathcal{T}$. Set $\mathbf{a}_\kappa^t = [\mathbf{a}^t \mid \mathbf{a}_0^t + \sum_{i=1}^d \kappa_i \mathbf{a}_i^t]$, where κ_i denotes the i th bit of κ . Compute $\sigma \leftarrow \text{PreSample}(\mathbf{a}_\kappa^t, (\mathbf{R}^t, \mathbf{0})^t, u + \mathbf{d}^t \mathbf{m}, s)$. Output (κ, σ) .
- `Vrfy`($\text{pk}, \mathbf{m}, (\kappa, \sigma)$): If $\mathbf{a}_\kappa^t \sigma = u + \mathbf{d}^t \mathbf{m}$ and $\|\sigma\| \leq \beta$ and $\kappa \in \mathcal{T}$, output 1.

We claim security of the signature scheme as follows.

Theorem 8. *For every ppt adversary \mathcal{A} that makes at most $Q \leq 2^{\alpha(n)}$ signature queries and has EUF-CMA advantage ϵ , there exists an adversary \mathcal{B} against $\text{RSIS}_{\mathcal{R}_q, m, q, \beta'}$ with advantage $\left(\frac{\epsilon}{4Q^2}\right)^c (\epsilon(n)/2 - \text{negl}(n))^{\alpha/(\alpha-1)} \cdot \exp(-\pi\alpha) - 2^{-\Omega(n)}$, where $\beta' = n^{7/2} \cdot \log n \cdot \omega(\log n)^{5/2}$, for any $\alpha > 1$.*

We now describe how one can change the proof of [DM14] in order to get adaptive security directly. In their proof, [DM14] can already answer all signature queries adaptively, except for at most one, since they know a trapdoor for the corresponding \mathbf{a}_κ^t . Only if there exists a query j such that $\kappa_{\leq i^*}^{(j)} = \kappa_{\leq i^*}^*$, i.e. if there exists a query j where the i^* bit long prefix of the j th tag $\kappa^{(j)}$ is the same as the guessed prefix $\kappa_{\leq i^*}^*$, there is no trapdoor. Thus [DM14] generate the signature answer σ^* not with a trapdoor but through other means, for which they need the non-adaptiveness. We change how we generate σ^* in this case and some other public values and analyse the changes. In the beginning, when given an RSIS instance $\mathbf{a}^t \in \mathcal{R}_q^{1 \times m_1}$, we choose the tags $\kappa^{(1)}, \dots, \kappa^{(Q)}$ to be used in the signature queries. Then, we generate \mathbf{d}^t by choosing $\mathbf{U} \leftarrow \mathcal{R}_{\pm 1}^{m_1 \times m_2}$ and setting $\mathbf{d}^t = \mathbf{a}^t \mathbf{U}$. We define an index i^* and guess a prefix $\kappa_{\leq i^*}^* \leftarrow T_{i^*}$ as in [DM14]. Furthermore, if a j exists such that $\kappa_{\leq i^*}^{(j)} = \kappa_{\leq i^*}^*$, we generate u by choosing $\mathbf{e} \leftarrow D_{\mathcal{R}, s}^{m_1 + \zeta}$ and setting $u = \mathbf{a}_{\kappa^{(j)}}^t \mathbf{e}$. Then, in the j th query, if $\kappa_{\leq i^*}^{(j)} = \kappa_{\leq i^*}^*$ holds, we answer with $\mathbf{e}' = \mathbf{e} + \mathbf{d}$, where $\mathbf{d} = \begin{bmatrix} \mathbf{U} \mathbf{m} \\ \mathbf{0} \end{bmatrix}$. If no such j exists, we proceed as in [DM14], so we only look at the case where such a j exists.

We now want to argue that these changes are indistinguishable to a ppt adversary. From [Bou+23, Lemma 2.8] we know that the distribution of $(\mathbf{a}^t, \mathbf{a}^t \mathbf{U})$ is statistically close to uniform. Due to Lemma 8 we know that there exists a

transformation of \mathbf{a}^t to its normal form with probability $1 - 4q^{n/2}$. Then, with Corollary 7.4 of [LPR13b; LPR13a] we know that $(\mathbf{a}^t, \mathbf{a}^t \mathbf{e})$ is statistically close to uniform since $s > 2nq^{1/m_1+2/(nm_1)}$. Thus, we lastly have to argue about the distribution of \mathbf{e}' . We will argue that the distribution of \mathbf{e}' is statistically indistinguishable from the signature in the real game, when both are conditioned on the respective values of $\mathbf{a}^t, \mathbf{d}^t, u$. Then, we know that the joint distribution of \mathbf{pk} together with \mathbf{e}' is statistically indistinguishable. Let \mathbf{z} be some solution to $\mathbf{a}_{\kappa(j)}^t \mathbf{z} = \mathbf{u}$. Then, we know that in the original game the distribution of the j th signature σ_j conditioned on \mathbf{pk} is $D_{A^\perp(\mathbf{a}_{\kappa(j)}^t) + \mathbf{z} + \mathbf{d}, s} = D_{A^\perp(\mathbf{a}_{\kappa(j)}^t), s, -\mathbf{z} - \mathbf{d} + \mathbf{z} + \mathbf{d}}$. If we look at the distribution of \mathbf{e} conditioned on the \mathbf{pk} generated by \mathcal{B} , we see that its distribution is $D_{A^\perp(\mathbf{a}_{\kappa(j)}^t) + \mathbf{z}, s}$. Thus, the distribution of \mathbf{e}' is $D_{A^\perp(\mathbf{a}_{\kappa(j)}^t) + \mathbf{z}, s + \mathbf{d}} = D_{A^\perp(\mathbf{a}_{\kappa(j)}^t), s, -\mathbf{z} + \mathbf{z} + \mathbf{d}}$ and the distributions of σ_j and \mathbf{e}' only differ in their center. Therefore, from [LSS14, Lemma 4.2] we know that the Rényi difference of the two distributions is smaller than $\exp(\alpha\pi \|\mathbf{d}\|_2^2 / s^2) \leq \exp(\alpha\pi)$ for any $\alpha > 0$, where the latter holds by construction. Then, it holds that $\Pr[W_{i^*}]^{\alpha/(\alpha-1)} \leq \exp(\alpha\pi \|\mathbf{d}\|_2^2 / s^2) \Pr[W_{\mathbf{e}'}]$ by [LSS14, Lemma 4.1], where W_{i^*} is the event that the signature adversary outputs a valid forgery when given σ_{i^*} in the simulation (with changed public keys) and $W_{\mathbf{e}'}$ is the event that the signature adversary outputs a valid forgery when given \mathbf{e}' . The rest of the proof works as in [DM14]. Thus, together with the analysis from [DM14] we know that the probability $\gamma(n)$ that the RSIS adversary outputs a valid solution is

$$\begin{aligned} \gamma(n) &\geq \frac{1}{|T_{i^*}|} (\epsilon(n)/2 - \text{negl}(n))^{\alpha/(\alpha-1)} \cdot \exp(-\pi\alpha) - 2^{-\Omega(n)} \\ &\geq \left(\frac{\epsilon}{4Q^2}\right)^c (\epsilon(n)/2 - \text{negl}(n))^{\alpha/(\alpha-1)} \cdot \exp(-\pi\alpha) - 2^{-\Omega(n)}, \end{aligned}$$

where negl is a negligible function and c is defined as in [DM14]. Thus, we get adaptive security without having to use chameleon hashes at the cost of some reduction loss introduced by the Rényi divergence.

To prove the possession of a secret message-signature pair, we first rewrite the equation from the signature verification to

$$\left[\mathbf{a}^t \mid \mathbf{a}_0^t + \sum_{i=1}^d \kappa_i \mathbf{a}_i^t \right] \sigma = u + \mathbf{d}^t \mathbf{m} \Leftrightarrow \left[\mathbf{a}^t \mid \mathbf{a}_0^t \mid \mathbf{a}_1^t \mid \dots \mid \mathbf{a}_d^t \mid -\mathbf{d}^t \right] \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \kappa_1 \sigma_2 \\ \vdots \\ \kappa_d \sigma_2 \\ \mathbf{m} \end{pmatrix} = u,$$

where $\sigma = (\sigma_1^t, \sigma_2^t)^t$. Therefore, we have an equation that is quadratic in the secret and can thus be proven in the framework of [LNP22b]. To finish proving possession of a secret message-signature pair we additionally need to prove that σ is short and that κ, \mathbf{m} are bit vectors, which is also possible in the framework, thus we can instantiate the proof as shown in Table 4.

variable	description	instantiation
ϕ	# of equations to prove	1
ϕ_{eval}	# of evaluations with const. coeff. zero	0
v_e	# of exact norm proofs	1
v_d	# of non-exact norm proofs	0
k_{bin}	length of the binary vector to prove	$d + m_\mu$
\mathbf{s}_1	committed message in the Ajtai part	$(\kappa, \sigma, \mathbf{m})$
\mathbf{m}	committed message in the BDLOP part	\emptyset (no message)
f_1	equation to prove	$\mathbf{a}_\kappa^t \sigma = u + \mathbf{d}^t \mathbf{m}$
\mathbf{E}_1	public matrix for proving $\ \mathbf{E}_1 \mathbf{s} - \mathbf{v}_1\ \leq \beta_1^{(e)}$	$[\mathbf{0} \ \mathbf{I} \ \mathbf{0}]$
\mathbf{v}_1	public vector for proving $\ \mathbf{E}_1 \mathbf{s} - \mathbf{v}_1\ \leq \beta_1^{(e)}$	$\mathbf{0}$
$\beta_1^{(e)}$	upper bound on $\ \mathbf{E}_1 \mathbf{s} - \mathbf{v}_1\ \leq \beta_1^{(e)}$	β
\mathbf{E}_{bin}	matrix for proving binary	$\text{diag}(\mathbf{I}, \mathbf{0}, \mathbf{I})$
\mathbf{v}_{bin}	vector for proving binary	0

Table 4. Proving possession of aucas-Micciancio signature (κ, σ) of a message \mathbf{m} .

C Stateful Lattice Signatures

Before constructing stateful lattice signatures, we first need some additional preliminaries.

Definition 28 (MSIS). *Let $q > 2$ and $d, m, \beta > 0$. Let \mathcal{R} be a ring and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. The MSIS problem $\text{MSIS}_{q, \mathcal{R}, d, m, \beta}$ is given a uniform matrix $\mathbf{A} \leftarrow \mathcal{R}_q^{d \times m}$ to find a non-trivial vector $\mathbf{x} \in \mathcal{R}_q^m \setminus \{\mathbf{0}\}$ such that $\mathbf{A}\mathbf{x} = \mathbf{0}$ and $\|\mathbf{x}\| \leq \beta$.*

For the MSIS problem there exists a so-called normal-form variant, where if $m > d$ the first d columns of \mathbf{A} form the identity matrix.

We can analyze the probability that we can transform an MSIS instance into a normal-form instance and vice-versa.

Lemma 8. *Let n, q and ring \mathcal{R}_q be as in the previous lemma. If matrix $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2]$, $\mathbf{A}_1 \in \mathcal{R}_q^{k \times k}$, $\mathbf{A}_2 \in \mathcal{R}_q^{k \times (n-k)}$, is chosen uniformly at random from $\mathcal{R}_q^{k \times n}$, $n \geq k$, then with probability at least $1 - 4k \cdot q^{-n/2}$, there is a matrix \mathbf{A}'_2 such that for $\mathbf{A}' = [\mathbf{I}_k | \mathbf{A}'_2]$*

$$\Lambda^\perp(\mathbf{A}) = \Lambda^\perp(\mathbf{A}').$$

The proof for this lemma can be found in Appendix D.

To present our construction of a stateful ℓ -time reputation system, we need stateful ℓ -time signatures, as we use them as a building block. We first define the formal model of such a signature.

Definition 29 (Stateful Signature Scheme). *A stateful ℓ -time signature scheme Σ consists of the following ppt algorithms:*

- $\text{KeyGen}(1^n)$ outputs secret key and public key pair (sk, pk) and a state st .

- $\text{Sign}(\text{sk}, m, st)$ outputs signature σ and state st' .
- $\text{Vrfy}(\text{pk}, m, \sigma)$ is deterministic and outputs a bit.

We say that Σ is correct if for all $n \in \mathbb{N}$, all $(\text{sk}, \text{pk}, st_1)$ output by $\text{KeyGen}(1^n)$, all messages m_1, \dots, m_ℓ , all $1 \leq i \leq \ell$, and all (st_{i+1}, σ_i) output by $\text{Sign}(\text{sk}, m_i, st_i)$, we have $\text{Vrfy}(\text{pk}, m_i, \sigma_i) = 1$. We additionally require that for all $1 \leq i \leq \ell$ we have that $|st_i| \leq p(n)$ for some polynomial p .

To define the EUF-CMA security of a stateful scheme in comparison to a standard stateless EUF-CMA definition, we simply define the signature oracle to remember the (updated) state in between its calls.

Definition 30 (Stateful EUF-CMA). A stateful ℓ -time signature scheme Σ is existentially unforgeable under chosen-message attacks (stateful-EUF-CMA) if for all ppt \mathcal{A} that make at most ℓ oracle queries,

$$\text{Adv}_{II, \mathcal{A}}^{\text{SEUFCMA}}(n) = \Pr[\text{Vrfy}(\text{pk}, m^*, \sigma^*) = 1 \wedge \mathcal{A} \text{ has not queried } m : (\text{sk}, \text{pk}, st_1) \leftarrow \text{KeyGen}(1^n), (m^*, \sigma^*) \leftarrow \mathcal{A}^{\text{SigO}(\text{sk}, \cdot)}(\text{pk})] \leq \text{negl}(n),$$

where $\text{SigO}(\text{sk}, m_i)$ is an oracle that computes $(\sigma_i, st_{i+1}) \leftarrow \text{Sign}(\text{sk}, m_i, st_i)$ on the i th query, and returns σ_i .

C.1 Stateful Signatures Based on Module SIS

The first construction of a stateful ℓ -time signature scheme is based on Module SIS and works similar to the construction of [JRS23]. In comparison to their construction, we do not commit to the message before signing it, which allows us to simplify the construction and the security proof.

Construction 31. Let $q \geq 2$ with $q = 5 \pmod 8$ be an odd prime and let $\zeta, m_3 > 0$. Let $m_1 = k \log q + \omega(\log n)$ and $m_2 = k\zeta$. Let $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$ and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let the message space be $\mathcal{R}_2^{m_3} \setminus \{\mathbf{0}\}$. Let $g = \lceil q^{\frac{1}{\zeta}} \rceil$, $\mathbf{g} = [1 \mid g \mid \dots \mid g^{\zeta-1}]$, and $\mathbf{G} = \mathbf{I}_d \otimes \mathbf{g} \in \mathcal{R}_q^{k \times m_2}$. Let $s = \eta_\epsilon(\mathbb{Z}) \sqrt{1+g^2} \sqrt{1+(\sqrt{nm_1} + \sqrt{nm_2} + t)^2} > 2nq^{k/m_1+2/(nm_1)}$ large enough and $\beta = s\sqrt{n(m_1+m_2)}$ such that $s^2 \geq (\sqrt{nm_1} + \sqrt{nm_3} + t)\sqrt{nm_3}$. Let $\beta = s\sqrt{n(m_1+m_2)}$. Let $w > 0$ and $\mathcal{T}_w = \{e \in \mathcal{R}_2 : \|e\| = \sqrt{w}\}$. Assume there is some order on the elements of \mathcal{T}_w . Call κ_i the i th element of \mathcal{T}_w in this order.

- $\text{KeyGen}(1^n)$: Choose $\mathbf{A} \leftarrow \mathcal{R}_q^{k \times m_1}$. Choose $\mathbf{R} \leftarrow \mathcal{R}_{\pm 1}^{m_1 \times m_2}$. Choose $\mathbf{D} \leftarrow \mathcal{R}_q^{k \times m_3}$, $\mathbf{u} \leftarrow \mathcal{R}_q^n$. Set $\text{pk} = (\mathbf{A}, \mathbf{B} = \mathbf{A}\mathbf{R}, \mathbf{D}, \mathbf{u})$ and $\text{sk} = \mathbf{R}$. Set $st = \kappa_1$.
- $\text{Sign}(\text{sk}, st, \mathbf{m})$: Set $\mathbf{A}_{\kappa_i} = [\mathbf{A} \mid \mathbf{B} + \kappa_i \mathbf{G}]$ and compute $\sigma \leftarrow \text{PreSample}(\mathbf{A}_{\kappa_i}, -\mathbf{R}, \mathbf{u} + \mathbf{D}\mathbf{m}, s)$. Set $st' = \kappa_{i+1}$. Output $((\kappa, \sigma), st')$.
- $\text{Vrfy}(\text{pk}, \mathbf{m}, (\kappa, \sigma))$: If $\mathbf{A}_{\kappa}\sigma = \mathbf{u} + \mathbf{D}\mathbf{m}$ and $\|\sigma\| \leq \beta$ and $\kappa \in \mathcal{T}_w$, output 1.

Lemma 9. *For every ppt adversary that makes at most $|\mathcal{T}_w|$ signature queries and wins the stateful-EUF-CMA game with advantage $\gamma(n)$ against Construction 31, there exists a ppt adversary against $\text{MSIS}_{\mathcal{R}_q, k, m_1, q, \beta'}$, where*

$$\beta' = \sqrt{1 + (\sqrt{nm_1} + \sqrt{nm_2} + t)^2 \cdot (\beta + s\sqrt{n(m_1 + m_2)}) + (\sqrt{nm_1} + \sqrt{nm_3} + t)\sqrt{nm_3}},$$

with advantage $\frac{1}{|\mathcal{T}_w|}\gamma(n) - \text{negl}(n)$.

Proof. Since the construction is similar to the one of [JRS23], the proof is similar as well. However, our proof differs in some details.

Let \mathcal{A} be an adversary against the stateful-EUF-CMA security of the signature. From this we construct an adversary \mathcal{B} against MSIS as follows:

- On input $\mathbf{A} \in \mathcal{R}_q^{k \times m_1}$, \mathcal{B} chooses $i^* \leftarrow |\mathcal{T}_w|$. It then chooses $\mathbf{R} \leftarrow \mathcal{R}_{\pm 1}^{m_1 \times m_2}$ and $\mathbf{U} \leftarrow D_{\mathcal{R}_{\pm 1}}^{m_1 \times m_3}$ and $\mathbf{e} \leftarrow D_{\mathcal{R}, s}^{m_1 + m_2}$. It then sets $\mathbf{u} = \mathbf{A}_{\kappa^*} \mathbf{e}$ and $\mathbf{B} = \mathbf{A}\mathbf{R} - \kappa_{i^*} \mathbf{G}$ and $\mathbf{D} = \mathbf{A}\mathbf{U}$ and $\text{pk} = (\mathbf{A}, \mathbf{B}, \mathbf{D}, \mathbf{u})$.
- \mathcal{B} simulates \mathcal{A} on input pk . On the i th signature query with message \mathbf{m} , \mathcal{B} does the following:
 - If $i \neq i^*$, answer with $(\kappa_i, \text{Sign}(-\mathbf{R}, \kappa_i, \mathbf{m}))$.
 - If $i = i^*$, answer with $(\kappa_{i^*}, \mathbf{e}' = \mathbf{e} + \begin{bmatrix} \mathbf{U}\mathbf{m} \\ \mathbf{0} \end{bmatrix})$.
- \mathcal{A} outputs some forgery $(m^*, \kappa^*, \sigma^*)$. If $\kappa^* \neq \kappa_{i^*}$, abort.
- \mathcal{B} returns $\mathbf{w} = [\mathbf{I} \mid \mathbf{R}](\sigma^* - \mathbf{e}) - \mathbf{U}\mathbf{m}^*$.

First, we want to argue that the view of \mathcal{A} is correct. For that, we see that \mathbf{A} and the oracle answers in the case $i \neq i^*$ have the same distribution as in the original game. For $\mathbf{B}, \mathbf{D}, \mathbf{u}$ and the oracle answer in the case $i = i^*$ we see that they are computed differently. From [Bou+23, Lemma 2.8] we know that the distribution of $(\mathbf{A}, \mathbf{A}\mathbf{R}, \mathbf{A}\mathbf{U})$ is statistically close to uniform. Due to Lemma 8 we know that there exists a transformation of \mathbf{A} to its normal form with probability $1 - 4kq^{n/2}$. Then, with Corollary 7.4 of [LPR13b; LPR13a] we know that $(\mathbf{A}, \mathbf{A}\mathbf{e})$ is statistically close to uniform since $s > 2nq^{k/m_1 + 2/(nm_1)}$. Thus, we lastly have to argue about the distribution of the i^* th query answer. We will argue that the distribution of \mathbf{e}' is statistically indistinguishable from the signature in the real game, when both are conditioned on the respective values of $\mathbf{A}, \mathbf{B}, \mathbf{D}, \mathbf{u}$. Then, we know that the joint distribution of pk together with \mathbf{e}' is statistically indistinguishable. Let \mathbf{z} be some solution to $\mathbf{A}_{\kappa_{i^*}} \mathbf{z} = \mathbf{u}$. Let \mathbf{c} be some solution to $\mathbf{A}_{\kappa_{i^*}} \mathbf{c} = \mathbf{D}\mathbf{m}$. Let $\mathbf{d} = \begin{bmatrix} \mathbf{U}\mathbf{m} \\ \mathbf{0} \end{bmatrix}$. Then, we know that in the original game the distribution of the i^* th signature σ_{i^*} conditioned on pk is $D_{\Lambda^\perp(\mathbf{A}_{\kappa_{i^*}}) + \mathbf{z} + \mathbf{d}, s} = D_{\Lambda^\perp(\mathbf{A}_{\kappa_{i^*}}), s, -\mathbf{z} - \mathbf{d} + \mathbf{z} + \mathbf{d}}$. If we look at the distribution of \mathbf{e} conditioned on the pk generated by \mathcal{B} , we see that its distribution is $D_{\Lambda^\perp(\mathbf{A}_{\kappa_{i^*}}) + \mathbf{z}, s}$. Thus, the distribution of \mathbf{e}' is $D_{\Lambda^\perp(\mathbf{A}_{\kappa_{i^*}}) + \mathbf{z}, s} + \mathbf{d} = D_{\Lambda^\perp(\mathbf{A}_{\kappa_{i^*}}), s, -\mathbf{z} + \mathbf{z} + \mathbf{d}}$ and the distributions of σ_{i^*} and \mathbf{e}' only differ in their center. Therefore, from [LSS14, Lemma 4.2] we know that the Rényi difference of the two distributions is smaller than $\exp(\alpha\pi \|\mathbf{d}\|_2^2 / s^2)$. Then,

it holds that $\Pr[W_{i^*}]^{\alpha/(\alpha-1)} \leq \exp(\alpha\pi \|\mathbf{d}\|^2/s^2) \Pr[W_{\mathbf{e}'}]$ by [JRS23, Lemma B.1], where W_{i^*} is the event that \mathcal{A} outputs a valid forgery when given σ_{i^*} in the simulation (with changed public keys) and $W_{\mathbf{e}'}$ is the event that \mathcal{A} outputs a valid forgery when given \mathbf{e}' . Thus, we know that the probability $\gamma(n)$ that \mathcal{A} outputs a valid forgery in the stateful-EUF-CMA game is smaller than $\gamma(n) \leq \left(\exp(\alpha\pi \|\mathbf{d}\|^2/s^2) \Pr[W_{\mathbf{e}'}]\right)^{(\alpha-1)/\alpha} + \text{negl}(n)$.

What is left to argue is that \mathbf{w} is a valid MSIS solution if \mathcal{A} outputs a valid forgery. From the following equation we can see that \mathbf{w} is indeed a vector that maps to $\mathbf{0}$ for the MSIS challenge.

$$\begin{aligned} \mathbf{A}_{\kappa^*} \sigma^* &= \mathbf{u} + \mathbf{Dm}^* \wedge \mathbf{A}_{\kappa^*} \left(\mathbf{e} + \begin{bmatrix} \mathbf{Um}_{i^*} \\ \mathbf{0} \end{bmatrix} \right) = \mathbf{u} + \mathbf{Dm}_{i^*} \\ \Rightarrow \mathbf{A}_{\kappa^*} \sigma^* - \mathbf{Dm}^* &= \mathbf{A}_{\kappa^*} \left(\mathbf{e} + \begin{bmatrix} \mathbf{Um}_{i^*} \\ \mathbf{0} \end{bmatrix} \right) - \mathbf{Dm}_{i^*} \\ \Leftrightarrow [\mathbf{A} \mid \mathbf{AR}] \sigma^* - \mathbf{A} \mathbf{Um}^* &= [\mathbf{A} \mid \mathbf{AR}] \left(\mathbf{e} + \begin{bmatrix} \mathbf{Um}_{i^*} \\ \mathbf{0} \end{bmatrix} \right) - \mathbf{A} \mathbf{Um}_{i^*} \\ \Leftrightarrow \mathbf{A} \cdot ([\mathbf{I} \mid \mathbf{R}] (\sigma^* - \mathbf{e}) - \mathbf{Um}^*) &= \mathbf{0} \end{aligned}$$

Now, for \mathbf{w} to be a valid MSIS solution, it also must be non-zero and short. We follow the heuristic of [JRS23] for the spectral norms of \mathbf{R} and \mathbf{U} and bound them by $s_1(\mathbf{R}) \leq \sqrt{nm_1} + \sqrt{nm_2} + t$ and $s_1(\mathbf{U}) \leq \sqrt{nm_1} + \sqrt{nm_3} + t$ for some small t . If one wants to use provable bounds, see [JRS23, Section 6.2] for details. For the norm of \mathbf{e} one can show that using [MP12, Lemma 2.9] that $\|\mathbf{e}\| \leq s\sqrt{n(m_1 + m_2)}$ with overwhelming probability. Therefore, we know that

$$\begin{aligned} \|[\mathbf{I} \mid \mathbf{R}] (\sigma^* - \mathbf{e}) - \mathbf{Um}\| &\leq s_1([\mathbf{I} \mid \mathbf{R}]) (\|\sigma^*\| + \|\mathbf{e}\|) + s_1(\mathbf{U}) \|\mathbf{m}\| \\ &\leq \sqrt{1 + (\sqrt{nm_1} + \sqrt{nm_2} + t)^2} \cdot (\beta + s\sqrt{n(m_1 + m_2)}) \\ &\quad + (\sqrt{nm_1} + \sqrt{nm_3} + t) \sqrt{nm_3} \end{aligned}$$

To show that \mathbf{w} is non-zero, we rewrite $\mathbf{w} = \mathbf{y} - \mathbf{Um}$ for some \mathbf{y} . Since we restricted the message space to $\mathcal{R}_q^{m_3} \setminus \{\mathbf{0}\}$, we know that there is at least one column of \mathbf{U} that influences \mathbf{w} . Therefore, the adversary has to predict at least one column \mathbf{u}' of \mathbf{U} in order to somehow produce \mathbf{y}, \mathbf{m} such that $\mathbf{w} = \mathbf{0}$. The only places where the adversary might get information about \mathbf{U} from are $\mathbf{D} = \mathbf{AU}$ and $\mathbf{e}' = \mathbf{e} + \begin{pmatrix} \mathbf{Um} \\ \mathbf{0} \end{pmatrix} = \mathbf{e} + \mathbf{d}$. However, in a hypothetical game where an unbounded adversary \mathcal{C} tries to predict \mathbf{u}' from information obtained in the stateful-EUF-CMA game, we can gamehop the information about \mathbf{U} in \mathbf{e}' away by replacing \mathbf{e}' by a Gaussian sampled vector and analyze the probability of predicting a column \mathbf{u}' of \mathbf{U} given $\mathbf{D} = \mathbf{AU}$. Let V denote the view of \mathcal{C} in the

stateful-EUF-CMA game without \mathbf{D}, \mathbf{e}' .

$$\begin{aligned}
& \Pr[\mathbf{u}^* = \mathbf{u}' : \mathbf{u}^* \leftarrow \mathcal{C}(V, \mathbf{D}, \mathbf{e}'), \mathbf{e}' = \mathbf{e} + \mathbf{d}] \\
& \leq \left(\Pr[\mathbf{u}^* = \mathbf{u}' : \mathbf{u}^* \leftarrow \mathcal{C}(V, \mathbf{D}, \mathbf{e}''), \mathbf{e}'' \leftarrow D_{\mathcal{R}_q, s}] \cdot \exp(\alpha\pi \|\mathbf{d}\|^2 / s^2) \right)^{\frac{\alpha-1}{\alpha}} \cdot \frac{1+\epsilon}{1-\epsilon} \\
& \leq \left(\text{negl}'(n) \cdot \exp(\alpha\pi \|\mathbf{d}\|^2 / s^2) \right)^{\frac{\alpha-1}{\alpha}} \cdot \frac{1+\epsilon}{1-\epsilon} \\
& \leq \text{negl}(n)
\end{aligned}$$

Here, the first inequality follows from [LSS14, Lemma 4.2]. Note that we need the other direction than before, since here we go from a shifted Gaussian to a non-shifted Gaussian. The second inequality follows from [DRS04, Lemma 2.2]: Since there is one column in \mathbf{D} influenced by \mathbf{u}' , which has $q^{kn} = 2^{kn \log q}$ possible values, and \mathbf{u}' has Shannon entropy $H_\infty(\mathbf{u}') = \log(3^{m_1}) = m_1 \log_2(3)$, we have

$$\begin{aligned}
\tilde{H}_\infty(\mathbf{u}' \mid \mathbf{D}) & \geq H_\infty(\mathbf{u}') - kn \log q \\
& = (kn \log q + \omega(\log n)) \log_2(3) - kn \log q \\
& = (\log_2(3) - 1)kn \log q + \log_2(3)\omega(\log n).
\end{aligned}$$

Therefore, the probability of guessing a column of \mathbf{U} and thus the probability of $\mathbf{w} = \mathbf{0}$ are negligible. Thus, together with the analysis about the view of \mathcal{A} , we know that the probability that \mathcal{B} outputs a valid MSIS solution is greater than

$$\begin{aligned}
\Pr[\mathcal{B} \text{ wins}] & \geq (\gamma(n) - \text{negl}(n))^{\alpha/(\alpha-1)} \cdot \exp(-\alpha\pi \|\mathbf{d}\| / s^2) - \text{negl}(n) \\
& \geq (\gamma(n) - \text{negl}(n))^{\alpha/(\alpha-1)} \cdot \exp(-\alpha\pi) - \text{negl}(n)
\end{aligned}$$

where the last equation follows since $\|\mathbf{d}\| \leq (\sqrt{nm_1} + \sqrt{nm_3} + t)\sqrt{nm_3} < s^2$. \square

C.2 Stateful Signatures Based on RSIS, RLWE and NTRU

Our second construction of a stateful ℓ -time signature works similar to Construction 31 and thus to the construction of [JRS23], but is instead based on RSIS, RLWE and NTRU. Depending on whether it is advantageous to be based on MSIS instead of RSIS (i.e. depending on the required degree n of the underlying ring), this signature scheme can achieve greater efficiency than Construction 31. This is because the former signatures use a regularity lemma for hiding, while the latter signatures use RLWE to hide, which comes at the cost of also needing the NTRU assumption. We start with defining the NTRU problem.

Definition 32 (NTRU). *Let $q > 2$ and $s > 0$ and n be a power of two. Let $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$ and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. The NTRU problem $\text{NTRU}_{q, \mathcal{R}, s}$ is to distinguish between a uniform $h \leftarrow \mathcal{R}_q$ and $h = gf^{-1}$, where $f, g \leftarrow D_{\mathcal{R}, s}$ such that f is invertible.*

We now construct the signature scheme. Note that apart from some parameters and dimensions, the scheme is the same as Construction 31.

Construction 33. Let $q \geq 2$ be odd with $q = 5 \pmod{8}$ and $\zeta, m_3 > 0$. Let $\mathcal{R} = \mathbb{Z}[X]/(X^n+1)$ and $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$. Let the message space be $\mathcal{R}_2^{m_3} \setminus \{\mathbf{0}\}$. Let $g = \lceil q^{\frac{1}{\zeta}} \rceil$ and $\mathbf{g} = [1 \mid g \mid \dots \mid g^{\zeta-1}]$. Let $s = \eta_\epsilon(\mathbb{Z})\sqrt{1+g^2}\sqrt{1+(\sqrt{2n}+\sqrt{\zeta n}+t)^2} > 2nq^{1/2+n}$ large enough such that $s^2 \geq (\sqrt{2n} + \sqrt{nm_3} + t)\sqrt{nm_3}$. Let $\beta = s\sqrt{n(2+\zeta)}$. Let $w > 0$ and $\mathcal{T}_w = \{e \in \mathcal{R}_2 : \|e\| = \sqrt{w}\}$. Assume there is some order on the elements of \mathcal{T}_w . Call κ_i the i th element of \mathcal{T}_w in this order.

- **KeyGen**(1^n): Choose $a' \leftarrow \mathcal{R}_q$. Choose $\mathbf{R} \leftarrow \mathcal{R}_{\pm 1}^{2 \times \zeta}$. Choose $\mathbf{d} \leftarrow \mathcal{R}_q^{1 \times m_3}$, $u \leftarrow \mathcal{R}_q$. Set $\mathbf{a} = [1 \mid a'] \in \mathcal{R}_q^{1 \times 2}$. Set $\text{pk} = (\mathbf{a}, \mathbf{b} = \mathbf{a}\mathbf{R}, \mathbf{d}, u)$ and $\text{sk} = \mathbf{R}$. Set $st = \kappa_1$.
- **Sign**($\text{sk}, st, \mathbf{m}$): Set $\mathbf{a}_{\kappa_i} = [\mathbf{a} \mid \mathbf{b} + \kappa_i \mathbf{g}]$ and compute $\sigma \leftarrow \text{PreSample}(\mathbf{a}_{\kappa_i}, -\mathbf{R}, u + \mathbf{d}\mathbf{m}, s)$. Set $st' = \kappa_{i+1}$. Output (κ, σ, st') .
- **Vrfy**($\text{pk}, \mathbf{m}, (\kappa, \sigma)$): If $\mathbf{a}_\kappa \sigma = u + \mathbf{d}\mathbf{m}$ and $\|\sigma\| \leq \beta$ and $\kappa \in \mathcal{T}_w$, output 1.

Lemma 10. For every ppt adversary that makes at most $|\mathcal{T}_w|$ signature queries and wins the stateful-EUF-CMA game with advantage $\gamma(n)$ against Construction 33, there exists a ppt adversary against $\text{RSIS}_{q,\mathcal{R},2,\beta'}$, where

$$\beta' = \sqrt{1 + (\sqrt{2n} + \sqrt{\zeta n} + t)^2} \cdot (\beta + s\sqrt{n(2+\zeta)}) + s(\sqrt{2n} + \sqrt{nm_3} + t)\sqrt{nm_3},$$

with advantage greater than $\frac{1}{|\mathcal{T}_w|} \exp(-\alpha\pi) (\gamma(n) - \text{negl}(n))^{\alpha/(\alpha-1)} - \text{negl}(n)$, if $\text{RLWE}_{q,\mathcal{R},s}$ and $\text{NTRU}_{q,\mathcal{R},s'}$ are hard.

Proof. The proof works similarly to the one in the construction based on Module SIS by first puncturing the public key at a random tag τ^* , generating \mathbf{d} and u differently with secret information, such that the secret information helps with answering the signature query for τ^* . However, similar to the proof in [Che+19], we show that puncturing the key is indistinguishable to the adversary not by some regularity lemma, but by the RLWE assumption. To show this, we temporarily lose the \mathbf{R} , with which we generate the signature query answers. Instead we temporarily introduce an NTRU trapdoor to generate the answers.

We prove this formally with the following game hops. Let Game_0 be the original stateful-EUF-CMA game. Let $\gamma(n)$ be the probability that \mathcal{A} wins in this game. Let $\hat{\gamma}_i(n)$ be the probability that \mathcal{A} wins in Game_i .

Game_1 is the same game as Game_0 , except that a' is instead set to $a' = gf^{-1}$, where $g, f \leftarrow D_{\mathcal{R}_q, s'}$. This is indistinguishable by the $\text{NTRU}_{q,\mathcal{R},s'}$ assumption. Let $\gamma_{\text{NTRU}}(n)$ be the advantage of some ppt adversary against $\text{NTRU}_{q,\mathcal{R},s'}$. Then, we have that $|\hat{\gamma}_0(n) - \hat{\gamma}_1(n)| = \gamma_{\text{NTRU}}(n)$.

Game_2 is the same game as Game_1 , except that the signature query answers are generated with the NTRU trapdoor instead of \mathbf{R} . In particular, by knowing f, g we can construct a basis of the lattice defined by a' such that the norm of its orthogonalization is $1.17\sqrt{q}$ [DLP14]. Since $s \geq 1.17\sqrt{q} \cdot \omega(\sqrt{\log n})$, we can use the GPV preimage sampler [GPV08] to generate the signature query answers with a distribution that is statistically close to the distribution of the scheme. Therefore, we have that $|\hat{\gamma}_1(n) - \hat{\gamma}_2(n)| = \text{negl}(n)$

Game₃ is the same game as **Game₂**, except that $\mathbf{b} \leftarrow \mathcal{R}_q^\zeta$. Immediately, this is indistinguishable by the hardness of normal form $\text{RLWE}_{q,\mathcal{R},s}$. Let $\gamma_{\text{RLWE}}(n)$ be the advantage of some ppt adversary against $\text{RLWE}_{q,\mathcal{R},s}$. Then, we have $|\hat{\gamma}_2(n) - \hat{\gamma}_3(n)| = \gamma_{\text{RLWE}}(n)$.

Game₄ is the same game as **Game₃**, except that $\mathbf{b} = \mathbf{b}' - \kappa_{i^*} \mathbf{g}$, where $\mathbf{b}' \leftarrow \mathcal{R}_q^\zeta$ and $i^* \leftarrow |\mathcal{T}_w|$. This is indistinguishable since adding a constant to a uniform value does not change the distribution. Thus, we have $|\hat{\gamma}_3(n) - \hat{\gamma}_4(n)| = 0$.

Game₅ is the same game as **Game₄**, except that $\mathbf{b} = \mathbf{b}' - \kappa_{i^*} \mathbf{g}$, where $\mathbf{b}' = \mathbf{a}\mathbf{R} \in \mathcal{R}_q^\zeta$ and $\mathbf{R} \leftarrow \mathcal{R}_{\pm 1}^{2 \times \zeta}$. This is again indistinguishable due to the hardness of normal form $\text{RLWE}_{q,\mathcal{R},s}$ and we have $|\hat{\gamma}_4(n) - \hat{\gamma}_5(n)| = \gamma_{\text{RLWE}}(n)$.

Game₆ is the same game as **Game₅**, except that $u = [\mathbf{a} \mid \mathbf{b}]\mathbf{e}$ and $\mathbf{d} = \mathbf{a}\mathbf{R}'$, where $\mathbf{e} \leftarrow D_{\mathcal{R},s}^{2+\zeta}$ and $\mathbf{R}' \leftarrow D_{\mathcal{R},s}^{m_3 \times m_3}$. Since $s > 2nq^{1/2+n}$ we know from Corollary 7.4 of [LPR13b; LPR13a] that this is statistically indistinguishable. Thus, we have that $|\hat{\gamma}_5(n) - \hat{\gamma}_6(n)| = \text{negl}(n)$.

Game₇ is the same game as **Game₆**, except the i^* -th signature query is instead answered with $(\kappa_{i^*}, \mathbf{e}')$, where $\mathbf{e}' = \mathbf{e} + \begin{pmatrix} \mathbf{R}\mathbf{m} \\ \mathbf{0} \end{pmatrix}$. With a similar argument as in the proof for Lemma 9, we have $\hat{\gamma}_6(n) \leq (\exp(\alpha\pi \|\mathbf{d}\|/s^2) \hat{\gamma}_7(n))^{(\alpha-1)/\alpha} \leq (\exp(\alpha\pi) \hat{\gamma}_7(n))^{(\alpha-1)/\alpha}$, since $s^2 \geq (\sqrt{2n} + \sqrt{nm_3} + t)\sqrt{nm_3}$.

Game₈ is the same game as **Game₇**, except that on the i th signature query, if $i \neq i^*$, the answer is generated as in the original stateful-EUF-CMA game. With a similar argument as before, this is statistically indistinguishable. Thus, we have that $|\hat{\gamma}_7(n) - \hat{\gamma}_8(n)| = \text{negl}(n)$.

Game₉ is the same game as **Game₈**, except that $a' \leftarrow \mathcal{R}_q$ is chosen uniformly random instead. This is again indistinguishable by the $\text{NTRU}_{q,\mathcal{R},s'}$ assumption and we have $|\hat{\gamma}_8(n) - \hat{\gamma}_9(n)| = \gamma_{\text{NTRU}}(n)$.

Therefore, we know that we can simulate \mathcal{A} while having a public key punctured at κ_{i^*} . In total, we have the following.

$$\begin{aligned} \gamma(n) &= \hat{\gamma}_0(n) = \hat{\gamma}_0(n) \sum_{i=1}^6 -\hat{\gamma}_i(n) + \hat{\gamma}_i(n) \\ &\leq \gamma_{\text{NTRU}}(n) + 2\gamma_{\text{RLWE}}(n) + \text{negl}(n) + \hat{\gamma}_6(n) \\ &\leq \gamma_{\text{NTRU}}(n) + 2\gamma_{\text{RLWE}}(n) + \text{negl}(n) + (\exp(\alpha\pi) \hat{\gamma}_7(n))^{(\alpha-1)/\alpha} \\ &\leq \gamma_{\text{NTRU}}(n) + 2\gamma_{\text{RLWE}}(n) + \text{negl}(n) + \\ &\quad (\exp(\alpha\pi) (\gamma_{\text{NTRU}}(n) + \hat{\gamma}_9(n) + \text{negl}(n)))^{(\alpha-1)/\alpha} \end{aligned}$$

Now we can construct an adversary \mathcal{B} against RSIS that simulates \mathcal{A} in Game_9 : On input $\hat{\mathbf{a}} = [\hat{a}_1 \mid \hat{a}_2] \in \mathcal{R}_q^2$, it computes $\mathbf{a} = \hat{a}_1^{-1} \hat{\mathbf{a}}$, which is possible with probability $1 - q^{n/2}$ due to Lemma 8. It then simulates \mathcal{A} in Game_9 with that \mathbf{a} . When \mathcal{A} outputs a forgery $(m^*, \kappa^*, \sigma^*)$, \mathcal{B} outputs $\mathbf{w} = [\mathbf{I}_2 \mid \mathbf{R}](\sigma^* - \mathbf{e}) - \mathbf{R}' \mathbf{m}^*$.

Having defined this, we can show that with the same arguments as in the proof of Lemma 9, but with $k = 1$, that if \mathcal{A} outputs a valid forgery and the guess of i^* was correct, \mathbf{w} is an RSIS solution that is indeed valid, short and non-zero for \mathbf{a} with overwhelming probability. Then, we know that \mathbf{w} is also a valid, short, non-zero RSIS solution for $\hat{\mathbf{a}}$, since $\hat{\mathbf{a}} \mathbf{w} = \hat{a}_1 \mathbf{a} \mathbf{w} = \mathbf{0}$. Thus we have $\Pr[\mathcal{B} \text{ wins}] = \frac{1}{|\mathcal{T}_w|} \hat{\gamma}_9 - \text{negl}(n)$, where the negligible part is influenced by the probability that \hat{a}_1 is invertible and \mathbf{w} being non-zero and short.

In total this means \mathcal{B} solves $\text{RSIS}_{\mathcal{R}, q, 2, \beta'}$ with probability greater than

$$\Pr[\mathcal{B} \text{ wins}] \geq \frac{1}{|\mathcal{T}_w|} \exp(-\alpha\pi) (\gamma(n) - \gamma_{NTRU}(n) - 2\gamma_{RLWE}(n) - \text{negl}(n))^{\alpha/(\alpha-1)} - \gamma_{NTRU}(n) - \text{negl}(n)$$

□

D Normal-Form Module SIS

To prove security of the stateful signatures we construct in Appendix C, we need to be able to transform MSIS instances to normal-form instances. We present some technical lemmas that show us when this is possible. This may be of independent interest.

Lemma 11. *Let \mathcal{R} be a finite ring. We denote by*

$$\eta := \Pr[a \text{ not invertible} : a \leftarrow R]$$

the probability that an element chosen uniformly at random from R is not invertible. Then

$$\Pr[\mathbf{A} \text{ has a right-inverse} : \mathbf{A} \leftarrow \mathcal{R}^{k \times k}] \geq 1 - k \cdot \eta.$$

Proof. We prove the lemma by induction on k . For $k = 1$ the lemma is immediate from the definition of η . For the induction step, assume

$$\mathbf{A} = (a_{ij})_{1 \leq i, j \leq k}, \quad \text{where } a_{ij} \leftarrow \mathcal{R} \text{ for all } i, j.$$

By \mathbf{A}' denote the $(k-1) \times (k-1)$ submatrix of \mathbf{A} consisting of the last $k-1$ rows and columns of \mathbf{A} . By induction hypothesis applied to \mathbf{A}' with probability at least $1 - (k-1)\eta$ there exists a matrix \mathbf{T}' such that

$$\mathbf{A} \cdot \mathbf{T}' = \begin{bmatrix} a_{11} & * & \cdots & * \\ a_{21} & & & \\ \vdots & \mathbf{I}_{k-1} & & \\ a_{k1} & & & \end{bmatrix}.$$

By further column operations, i.e. another matrix \mathbf{T}'' , we can further modify \mathbf{A} to obtain

$$\mathbf{A} \cdot \mathbf{T}' \cdot \mathbf{T}'' = \begin{bmatrix} a_{11} + \gamma(\mathbf{A} \setminus \{a_{11}\}) * \cdots * \\ 0 \\ \vdots \\ \mathbf{I}_{k-1} \\ 0 \end{bmatrix},$$

where $\gamma(\mathbf{A} \setminus \{a_{11}\})$ is a term that depends on the entries in \mathbf{A} *except* a_{11} . Since a_{11} is chosen uniformly and independently (from entries in $\mathbf{A} \setminus \{a_{11}\}$) at random,

$$\Pr[a_{11} + \gamma(\mathbf{A} \setminus \{a_{11}\}) \text{ is not invertible} : a_{11} \leftarrow \mathcal{R}] \leq \eta.$$

If $a_{11} + \gamma(\mathbf{A} \setminus \{a_{11}\})$ is invertible, then there exists a matrix \mathbf{T}''' with

$$\mathbf{A} \cdot \mathbf{T}' \cdot \mathbf{T}'' \cdot \mathbf{T}''' = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 \\ \vdots & \mathbf{I}_{k-1} \\ 0 \end{bmatrix},$$

i.e. $\mathbf{T} = \mathbf{T}' \cdot \mathbf{T}'' \cdot \mathbf{T}'''$ is a right-inverse for \mathbf{A} . Summarizing,

$$\begin{aligned} \Pr[\mathbf{A} \text{ does not have a right-inverse} : \mathbf{A} \leftarrow \mathcal{R}^{k \times k}] &\leq \\ \Pr[\mathbf{A}' \text{ does not have a right-inverse} : \mathbf{A}' \leftarrow \mathcal{R}^{(k-1) \times (k-1)}]_+ & \\ \Pr[a_{11} + \gamma(\mathbf{A} \setminus \{a_{11}\}) \text{ is not invertible} : a_{11} \leftarrow \mathcal{R}] &\leq k \cdot \eta, \end{aligned}$$

which proves the lemma. □

The same arguments as in the previous proof can be applied to left-inverses and row operations, we obtain

Corollary 3. *With the assumptions and notation as in the previous lemma,*

$$\Pr[\mathbf{A} \text{ has a right- and a left-inverse} : \mathbf{A} \leftarrow \mathcal{R}^{k \times k}] \geq 1 - 2k \cdot \eta.$$

Lemma 12. *Let \mathcal{R} and η be as above. Assume matrix $\mathbf{A} = [\mathbf{A}_1 \mid \mathbf{A}_2]$, $\mathbf{A}_1 \in \mathcal{R}^{k \times k}$, $\mathbf{A}_2 \in \mathcal{R}^{k \times (n-k)}$, is chosen uniformly at random from $\mathcal{R}^{k \times n}$, $n \geq k$. Then with probability at least $1 - 2k \cdot \eta$, there is a matrix \mathbf{A}'_2 such that for $\mathbf{A}' = [\mathbf{I}_k \mid \mathbf{A}'_2]$*

$$\Lambda^\perp(\mathbf{A}) = \Lambda^\perp(\mathbf{A}').$$

Proof. By the previous corollary, over the choice of \mathbf{A} with probability $1 - 2k\eta$ matrix \mathbf{A}_1 has a left- and a right-inverse. As is well-known, if left- and right-inverses exist, then they are identical. Denote this inverse of \mathbf{A}_1 by \mathbf{A}_1^{-1} and set

$$\mathbf{A}' = \mathbf{A}_1^{-1} \cdot \mathbf{A} = [\mathbf{A}_1^{-1} \cdot \mathbf{A}_1 \mid \mathbf{A}_1^{-1} \cdot \mathbf{A}_2] = [\mathbf{I}_k \mid \mathbf{A}_1^{-1} \cdot \mathbf{A}_2].$$

We claim that $\Lambda^\perp(\mathbf{A}) = \Lambda^\perp(\mathbf{A}')$. Since $\mathbf{A} \cdot \mathbf{v} = 0$ implies $\mathbf{A}' \cdot \mathbf{v} = 0$, the inclusion $\Lambda^\perp(\mathbf{A}) \subseteq \Lambda^\perp(\mathbf{A}')$ follows. The other inclusion follows analogously by observing that

$$\mathbf{A}_1^{-1} \cdot \mathbf{A}' = \mathbf{A}_1 \cdot \mathbf{A}_1^{-1} \cdot \mathbf{A} = \mathbf{A}.$$

□

Next we apply this result to rings $\mathbb{Z}_q[X]/(X^n + 1)$ for relevant choices of n and q . To do so we use the following lemma.

Lemma 13. *Let n be a power of 2 and $q \geq 16$ a prime with $q \equiv 3, 5 \pmod{8}$. For the ring $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ with $\mathcal{R} := \mathbb{Z}[X]/(X^n + 1)$ we have*

$$\eta := \Pr[a \text{ not invertible} : a \leftarrow \mathcal{R}_q] \leq \frac{2}{q^{n/2}}.$$

Proof. For n, q as in the lemma, the polynomial $X^n + 1$ is irreducible over \mathbb{Q} and splits into two irreducible polynomials of degree $n/2$ modulo q . Hence

$$\mathcal{R}_q \cong \mathbb{F}_{q^{n/2}} \times \mathbb{F}_{q^{n/2}},$$

where $\mathbb{F}_{q^{n/2}}$ denotes the field with $q^{n/2}$ elements. Therefore non-invertible elements (zero-divisors and 0) in \mathcal{R}_q are of the form $(0, z)$ or $(z, 0)$ for $z \in \mathbb{F}_{q^{n/2}}$. Hence the number of non-invertible elements is $2q^{n/2} - 1$ and the lemma follows. □

Combining this lemma together with Lemma 12 then proves Lemma 8.

E Standard Security Definitions

E.1 Encryption Schemes

To construct our reputation system, we need a CPA secure encryption scheme as a building block. For this, we consider a standard syntax definition.

Definition 34. *An encryption scheme Π consists of the following three ppt algorithms.*

- $\text{KeyGen}(1^n)$: *The key generation algorithm on input a security parameter n outputs a tuple of a secret key and a public key (sk, pk) .*
- $\text{Enc}(\text{pk}, m)$: *The encryption algorithm on input a public key pk and a message m outputs a ciphertext c .*
- $\text{Dec}(\text{sk}, c)$: *The decryption algorithm on input a secret key sk and a ciphertext c outputs a message m .*

We say that Π is correct, if for all security parameters n , all (sk, pk) output by $\text{KeyGen}(1^n)$, and all messages m , it holds that $\Pr[\text{Dec}(\text{sk}, \text{Enc}(\text{pk}, m)) = m]$ is overwhelming in n .

We define CPA security with a standard definition as well.

IND-CPA _{Π, \mathcal{A}, b} (n)	
1:	$(\mathbf{sk}, \mathbf{pk}) \leftarrow \text{KeyGen}(1^n)$
2:	$(m_0, m_1) \leftarrow \mathcal{A}(\mathbf{pk})$
3:	$c \leftarrow \text{Enc}(\mathbf{pk}, m_b)$
4:	$b' \leftarrow \mathcal{A}(c)$

Definition 35. We define the advantage of an adversary \mathcal{A} against an encryption scheme Π as

$$\text{Adv}_{\Pi, \mathcal{A}}^{\text{CPA}}(n) = |\Pr[\text{IND-CPA}_{\Pi, \mathcal{A}, 0}(n) = 1] - \Pr[\text{IND-CPA}_{\Pi, \mathcal{A}, 1}(n) = 1]|.$$

We say that the scheme Π is IND-CPA secure if for all ppt adversaries $\text{Adv}_{\Pi, \mathcal{A}}^{\text{CPA}}(n)$ is negligible.

E.2 Signature Schemes

Another building block we need for the reputation system is an EUF-CMA secure signature scheme.

Definition 36 (Signature scheme). A signature scheme Σ consists of the following ppt algorithms:

- $\text{KeyGen}(1^n)$ outputs secret key and public key pair $(\mathbf{sk}, \mathbf{pk})$.
- $\text{Sign}(\mathbf{sk}, m)$ outputs signature σ .
- $\text{Vrfy}(\mathbf{pk}, m, \sigma)$ is deterministic and outputs a bit.

We say that Σ is correct if for all $n \in \mathbb{N}$, all $(\mathbf{sk}, \mathbf{pk})$ output by $\text{KeyGen}(1^n)$, all messages m in the message space (which is implicitly defined by the \mathbf{pk}), and all σ output by $\text{Sign}(\mathbf{sk}, m)$, we have $\text{Vrfy}(\mathbf{pk}, m, \sigma) = 1$.

The standard EUF-CMA security notion is defined as follows.

Definition 37 (EUF-CMA). A signature scheme Σ is existentially unforgeable under chosen-message attacks (EUF-CMA) if for all ppt \mathcal{A} ,

$$\begin{aligned} \text{Adv}_{\Pi, \mathcal{A}}^{\text{EUF-CMA}}(n) &= \Pr[\text{Vrfy}(\mathbf{pk}, m^*, \sigma^*) = 1 \wedge \mathcal{A} \text{ has not queried } m^* : \\ &\quad (\mathbf{sk}, \mathbf{pk}) \leftarrow \text{KeyGen}(1^n), (m^*, \sigma^*) \leftarrow \mathcal{A}^{\text{Sign}(\mathbf{sk}, \cdot)}(\mathbf{pk})] \leq \text{negl}(n). \end{aligned}$$