Many-time Linkable Ring Signatures

Nam Tran[1,2] *, Khoa Nguyen[1], Dongxi Liu[2],
Josef Pieprzyk[2,3], and Willy Susilo[1] **

[1] University of Wollongong, Northfields Avenue, Wollongong, NSW 2522, Australia
ndt141@uowmail.edu.au, khoa@uow.edu.au, wsusilo@uow.edu.au
[2] CSIRO Data61, Marsfield, 26 Pembroke Road, NSW 2122, Australia
[3] Institute of Computer Science, Polish Academy of Sciences, Poland
Dongxi.Liu@data61.csiro.au, Josef.Pieprzyk@data61.csiro.au

Abstract. Linkable ring signatures (Liu *et al.*, ACISP'04) is a ring signature scheme with a linking mechanism for detecting signatures from the same signer. This functionality has found many practical applications in electronic voting, cryptocurrencies, and whistleblowing systems. However, existing linkable ring signature schemes impose a fundamental limitation: users can issue only one signature, and after that their anonymity is not guaranteed. This limited number of usage is inadequate for many real-world scenarios.

This work introduces the notion of *Many-time Linkable Ring Signatures*, extending the anonymity guarantees of standard linkable ring signatures. Specifically, many-time linkable ring signatures ensure that signers remain anonymous as long as the number of their signatures is smaller than a system-global threshold. Only when a signer exceeds this threshold the anonymity is lost. We formalize this via a security notion called T-anonymity, which guarantees that adversaries cannot distinguish signatures from users who have each produced at most T signatures. This new notion of anonymity generalizes one-time anonymity in previous linkable schemes, while providing stronger guarantees than existing constructions. We also present a lattice-based construction with proven security in the quantum random oracle model (QROM).

1 Introduction

Ring signatures, proposed by Rivest *et al.* [49], are privacy-preserving signature systems that allow users to sign a message while concealing their identities among a group of signers. Since its introduction, there has been extensive research proposing many constructions from number-theoretic assumptions[1,8,51,6], post-quantum assumptions [35,26,7,43] and even from symmetric primitives [31].

Beyond privacy protection, researchers have incorporated many advanced functionalities in ring signatures. For example, threshold ring signatures [14]

* Nam Tran is supported by CSIRO Data61 PhD Scholarship and CSIRO Data61 Top-up Scholarship.
** Willy Susilo is supported by the Australian Research Council Australian Laureate Fellowship FL230100033.

generalize ring signatures by allowing many users to sign messages jointly. Accountable ring signatures [58] are another notable variant of ring signatures, where there is an authority that can trace signatures back to signers, essentially similar to the opening authority in group signatures [21].

Additional functionalities beyond privacy protection enable ring signatures to address situations where both anonymity and accountability must be balanced, as users with excessive anonymity can conduct illegal activities or suspicious actions against the designated purpose of the system. For that reason, mechanisms providing accountability in ring signatures are particularly desirable. One such mechanism is *linkability*, introduced in the notion of *linkable ring signatures* (LRS) [39]. Specifically, multiple signatures, if created by the same signer, can be detected, i.e., *linked*. Ring signatures, when equipped with such functionality, find various practical applications:

- Electronic-voting [23]: under a linkable ring signature scheme, each voter signs its ballot paper not only under its identity but also under the identities of all eligible voters, thus keeping voter's identity secret. At the same time, linkability prevents the voter from casting multiple ballots;
- Cryptocurrencies: some cryptocurrency systems (e.g., Monero [48]), employ linkable ring signatures to safeguard against double spending;
- Whistleblowing: the intended application of ring signatures is an anonymous whistleblowing system where users can secretly disclose information but still guarantee legitimacy. With linkability, the system can also detect if the user is making multiple reports (for assessing credibility), or prevent spam.

There has been active research into LRS since the foundational work of Liu *et al.* [39]. Similar to standard ring signatures, many constructions of LRS have been proposed, mostly from number-theoretic assumptions [39,56,30,62,65,11]. Recently, post-quantum constructions have been suggested, including lattice-based schemes of [5,40,41,3,7], isogeny-based designs of [7], code-based constructions of [12,13], and the proposal of [59] which is based on collision-resistant hash functions. Interestingly, besides linking, several of those works also offered additional functionalities:

- The work of [40] combines a linkable ring signature with a key derivation mechanism for generating stealth address, which more precisely captures privacy and security requirements in cryptocurrency systems;
- The LRS scheme of [65] offers a revoking mechanism similar to that of group signatures [21]. Namely, there is an authority that can trace a signature back to its signer;
- The LRS scheme of [30] offers a tracing mechanism in the following sense: whenever a secret key is used for signing twice on different messages, the tracing algorithm returns the corresponding public key.

Among the aforementioned constructions, the notion of linkability also varies. For instance, in the construction of [30], signatures on the same message and created under the same key are linked. In contrast, the constructions of [56,12,11]

employed *event-oriented* linking. Roughly speaking, the signature contains a component called *event-id*, and signatures with the same event-id and created under the same key are linked.

Nevertheless, in most linkable schemes, signatures can be linked if they originate from the same signing key, effectively limiting users to signing only once. Although there exists a different notion of anonymity [3,7], which does not restrict the number of messages users can sign. This notion, called *linkable anonymity*, however, puts another restriction on honest signers. Informally, they should always stay together in some ring.

The *one-time* limit on the number of usages in many linkable schemes turns out to be inadequate in certain situations. For instance, in trial-using systems or limited-time services, typically there is a global usage threshold due to systems' constraints. At the same time, users should have the right to privately access content multiple times, rather than being restricted to a single use. Another scenario is protection of online services against coordinated attacks such as denial-of-service or Sybil-type [25]. Allowing a limited number of anonymous actions rather than just one can potentially serve as a countermeasure, while maintaining reasonable system accessibility.

A more direct example in the context of LRS is electronic voting, where voters are allowed to cast multiple ballots (e.g., multiple-round voting). In this situation, standard LRS cannot apply, as users cannot cast additional ballots without being detected via the linking mechanism. Likewise, in online bidding or e-commerce platforms, while anonymity from ring signatures protects users from unfair competitors' strategy (intimidation, retaliation), standard linkability only provides single usage, thereby forbidding users from submitting multiple bids without compromising their anonymity.

Contributions and Techniques. We introduce the notion of *Many-time Linkable Ring Signatures* and provide a lattice-based construction with security proven in the quantum random oracle model (QROM). The notion extends anonymity in standard linkable ring signatures by allowing signers to stay completely anonymous if the number of signatures stays below certain threshold value T, where $\mathsf{T} \geq 1$ can be any polynomial in the security parameter. On the other hand, if signers exceed this threshold, their anonymity is lost.

Informally, a many-times linkable ring signature, which we denoted as T-LRS, consists of five polynomial-time algorithms ($\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Link}$). Algorithm Setup generates the system's public parameters and a threshold value T, which determines the maximum number of signatures a user can issue before linkage occurs. Here, we retain the fundamental idea of linkable ring signatures by allowing a mechanism detecting whether a signing key is used more than T times. More formally, the link algorithm Link, in contrast to the original formulation in [39], now takes a set of $\mathsf{T}+1$ valid signatures for linkage.

The security requirements, similar to those of LRS, are *anonymity, unforgeability, linkability* and *non-frameability*. While unforgeability, linkability and non-frameability are defined in a spirit similar to previous works, a more careful treatment should be made when defining anonymity. As the intended usage of the

system is for a user to create up to T unlinked signatures, we define anonymity in a setting where an adversary attempts to distinguish signatures from certain users while observing only at most T signatures from each. We refer to this as T-anonymity.

From a certain perspective, T-anonymity generalizes the notion of *one-time* anonymity in previous LRS constructions, which only guarantee anonymity if users sign exactly once. The exceptions are the constructions of [3,7], which satisfy a stronger notion called *linkable anonymity*. This property guarantees the anonymity of honest users even when they sign more than once, provided that these users always *stay together* in some ring when issuing signatures. In contrast, our definition of T-anonymity does not put such a restriction on the user's choice of rings. In Appendix E, we argue that our lattice-based construction, which we outline next, still achieves linkable anonymity.

We now describe the high-level idea of our lattice-based T-LRS. The starting point is the accumulator-based ring signature scheme of [35]. In this construction, a signer's public-secret key pair corresponds to an output-input pair from an SIS-based one-way hash function [2]. For signing while hiding its public key in a ring R, a signer employs the lattice-based accumulator of [35] to accumulate all public keys in R, then produces a non-interactive zero-knowledge (NIZK) proof proving knowledge of an accumulated value, and knowledge of a SIS preimage of the public key. The NIZK layer is obtained from Stern's ZK framework [52] via Fiat-Shamir transform [28]. The anonymity and unforgeability of the scheme rely on the security of the accumulator, the one-wayness of the SIS-based hash function, and the zero-knowledge property of the NIZK argument system.

To upgrade the lattice-based scheme of [35] to a many-time linkable scheme, we recall that the common idea in some linkable schemes such as [39,62,11] is to include a tag value t in the signature derived from the user's secret. This way, if a signer uses the same secret to sign more than once, the tags in the signatures should collide and the signatures are linked. Additionally, the tag must have sufficient pseudo-randomness in order not to leak information about signers. In those constructions, pseudo-randomness of tags relied on certain computational assumptions, or on a pseudo-random function (PRF) family that is used for computing tags from signer's secret.

The idea of employing PRFs naturally generalizes to the case where $\mathsf{T}+1$ signatures are needed for linkage; namely, the tag is evaluated from a function that takes two inputs: the user's secret key and a *counter* that resets after T times. Similarly to the one-time case, if a signer signs more than T times using the same secret, among $\mathsf{T}+1$ signatures, there should exist two tags with colliding values. On the other hand, signing up to T times does not hurt anonymity, as the tags are pseudo-random values that virtually leak nothing about signer's secret.

In more detail, we modify the lattice-based ring signature of [35] as follows: user's public key, instead of being an output of SIS-based hash function, is now a KTX commitment [33] to a uniformly random vector $\mathbf{x} \in \mathbb{Z}_q^m$. The user's secret includes $\mathbf{x}$ and the commitment randomness. To compute the tag in the signature, we employ the BLMR lattice-based PRF [9]. To sign a message, the

user proceeds similarly to [35], but in addition, proves in zero-knowledge that: it has an opening to a KTX commitment accumulated in the ring, that it has the seed and the input of the PRF that outputs the tag, and that the input (the counter) only takes value in the range $\{0, 1, \ldots, \mathsf{T} - 1\}$.

Although the above statements can be proven in ZK under Stern's framework, the constant soundness of 2/3 in Stern's Σ-protocol requires $\mathcal{O}(\lambda)$ parallel repetitions to achieve a negligible soundness error. Therefore, to reduce the number of parallel repetitions, we rely of the ZK argument system of Yang *et al.* [61]. In comparison with Stern's Σ-protocol, Yang *et al.*'s system is a commit-and-prove Σ-protocol for lattice-based linear and quadratic relations and therefore, it can handle the defining relations underlying a user's signature in our construction. Additionally, its inverse polynomial soundness error only requires $\mathcal{O}(\lambda/\log \mathsf{poly}(\lambda))$ parallel repetitions to make the error negligibly small, thus improving a factor of order $\log \mathsf{poly}(\lambda)$. Finally, to achieve full quantum security, rather than Fiat-Shamir transform [28], we employ the generalized Unruh transformation [57,27] that can turn any special-sound, honest-verifier zero-knowledge Σ-protocols (which is the case of Yang *et al.* ZK argument) to a non-interactive proof system secure in the QROM.

Other Related Works. Privacy-preserving digital signatures is a research area attracting significant interest. The current literature contains numerous constructions, offering diverse functionalities that aims to at protect user's privacy and/or provide powerful tracing capability. There are a few examples:

- Group signatures [21], similar to ring signatures in the aspect that users can sign anonymously in a group but allow a tracing authority who can open signatures to their original signers. There are extensions of group signatures with mechanisms such as verifier local revocation [10]; accountable tracing [34], or group signatures with message-dependent opening [50];
- Ring signatures with advanced functionalities beyond linkability, such as user-controlled linkability [29], enabling users to choose which signatures can be linked;
- Attribute-based signatures [44], which extend ring signatures by allowing signers to create signatures as long as they have certain information (*attributes*) satisfying some system-dependent criteria;
- Signature systems with hybrid privacy/accountability that combines the features of both ring and group signatures [37,46,47,55]. In these signature systems, users have the flexibility to decide which of their personal information can be disclosed by the tracing authority.

In the past, several works addressed privacy systems where anonymity is compromised whenever users perform actions contradicting the system's rules. For instance, in anonymous credential systems [19], it is sometimes favorable to allow users to anonymously authenticate up to a bounded number of times, preventing rogue users from attacking the systems. This problem was formally addressed by k-times anonymous authentication (k-TAA) [54] and some related works such as [24,16]. Another relevant context is cryptocurrency/electronic cash. In electronic

cash systems [20,17] and confident transaction protocols [53,63], users attempting double-spending are detected and may have their identities revealed by a designated authority.

The notion of T-anonymity offered by many-time LRS is, in essence, similar to "threshold anonymity" in k-TAA. However, the simplicity of the construction may be beneficial in situations that do not require sophisticated features beyond anonymity and linkability. Additionally, many-time LRS enables applications in contexts where centralized authorities are undesirable or unavailable, and the relaxed constraint on the number of usages may pave way for applications where one-time LRS constructions are insufficient. Electronic cash systems with monitoring policy could be a natural application domain, where possible policies include monitoring the number of transactions per day (as in [16]), or tracking the number of coins spent with particular merchants (as in [18]). Furthermore, the decentralized nature of (many-time) LRS provides better transparency, compared to the centralized approaches in anonymous authentication and electronic cash systems.

Regarding anonymity in LRS, there is a recent work from Bultel and Olivier-Anclin [15] with a comprehensive review of existing linkable ring signature schemes. They pointed out that one-time anonymity and linkable anonymity [3] are fundamentally distinct notions. In particular, most existing schemes only satisfy one-time linkability and have not been analyzed in the linkable anonymity model. Although Bultel and Olivier-Anclin argued in favor of the fact that most one-time linkable schemes can achieve linkable anonymity, the limits imposed by these notions show that anonymity in linkable ring signatures could turn out to be insufficient for meaningful applications. Therefore, we leave as an interesting question whether there exists an anonymity model of linkable ring signatures putting reasonable restrictions on users.

Another independent and concurrent work of Choi *et al.* [22] discussed the notion of k-Linkable Ring Signatures (k-LRS). While both k-LRS and T-LRS extend standard linkable ring signatures to allow users to sign multiple times anonymously, they differ fundamentally in linking mechanism. Specifically, k-LRS employs *event-oriented linking* similar to [56,12,11], where the linking algorithm Link requires an event label e as an additional input and guarantees that $k+1$ signatures are linked *if and only if* they are generated under the same event label and the same signing key. In contrast, T-LRS disregards event label, and links signatures by detecting collisions between linkability tags. Therefore, in T-LRS, if there is linkage of $\mathsf{T}+1$ input signatures, then it is the case that *at least two signatures* are from the same signers. The strong linking guarantee in k-LRS targets the specific scenario of voting, where authorities must identify and revoke ballots from a voter who exceeded the k-vote limit. While such a guarantee is necessary for applications requiring more users' accountability, in other contexts like cryptocurrency or whistleblowing, strong linkability (in the sense of k-LRS) turns out to be less desirable and could affect users' privacy. Therefore, the relaxation of T-LRS can offer better privacy protection through ambiguity of linkage, meaning that a subset of two signatures can be confidently

attributed to some signer while the remaining signatures might not. This makes T-LRS better suited for scenarios where user privacy protection is paramount, at the cost of less precise violation detection. The trade-off between privacy and accountability becomes clearer when examining how Link functions in both constructions. In k-LRS, Link requires some linear algebra manipulation, while in T-LRS Link checks for collision in PRF-based tags. Additionally, k-LRS's event-oriented linkage enables more fine-grained control, whereas T-LRS enforces a global linkage policy for any users' activities.

Organizations. We introduce basic notations and recall some backgrounds on lattice-based cryptography in Section 2. We discuss the syntax and security requirements of many-time LRS in Section 3, then present a lattice-based construction in Section 4. Several technical materials are provided in the Appendix.

2 Preliminaries

2.1 Basic Notations

Vectors are treated as column vectors and denoted by bold, lower-case letters. Matrices are denoted by bold, upper-case letters. The coordinates of a vector are indexed in an array-like manner, starting from 1; for example, given an n-th dimensional vector $\mathbf{v}$, then $\mathbf{v} = (\mathbf{v}[1], \ldots, \mathbf{v}[n])$.

For $n \in \mathbb{N}$, we let $[n]$ denote the set $\{1, \ldots, n\}$. We let $\mathsf{bin}(n) \in \{0,1\}^{\lceil \log n \rceil}$ be the binary representation of n in little-endian, which satisfies $n = \mathsf{bin}(n)[1] + \mathsf{bin}(n)[2] \cdot 2 + \ldots + \mathsf{bin}(n)[\lceil \log n \rceil] \cdot 2^{\lceil \log n \rceil - 1}$. The function bin naturally extends to $\mathbb{Z}_q^n$: for $\mathbf{v} \in \mathbb{Z}_q^n$, $\mathsf{bin}(\mathbf{v}) = (\mathsf{bin}(\mathbf{v}[1]), \ldots, \mathsf{bin}(\mathbf{v}[n])) \in \{0,1\}^{n\lceil \log q \rceil}$, where $\mathsf{bin}(\mathbf{v}[i])$ corresponds to the unique integer $v_i' \in \{0, 1, \ldots, q-1\}$ such that $v_i' = \mathbf{v}[i] \bmod q$.

We recall the rounding function in the BLMR lattice-based PRF [9]. For integers q and p where $q \geq p \geq 2$, the function $\lfloor \cdot \rfloor_{p,q} : \mathbb{Z}_q \to \mathbb{Z}_p$ maps $x \in \mathbb{Z}_q$ to $i \in \mathbb{Z}_p$, where $i \cdot \lfloor q/p \rfloor$ is the largest multiple of $\lfloor q/p \rfloor$ that does not exceed x. For a vector $\mathbf{v} \in \mathbb{Z}_q^m$, we define $\lfloor \mathbf{v} \rfloor_{p,q}$ as the vector in $\mathbb{Z}_p^m$ obtained by rounding each coordinate of the vector individually.

The ℓ_2-norm and ℓ_∞-norm of $\mathbf{x} \in \mathbb{R}^n$ are denoted by $\|\mathbf{x}\|_2$ and $\|\mathbf{x}\|_\infty$. We write $x \leftarrow D$ when x is sampled from a probability distribution D. We also write $x \xleftarrow{\$} S$ to indicate that x is sampled uniformly at random from a set S. We denote by $\mathcal{A}(x; r)$ to to indicate that a probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$ takes x as input and r as its random coin.

2.2 Lattice Assumptions

We recall the Short Integer Solutions (SIS) and the Learning With Errors (LWE) problems.

Definition 2.1. *For $i \in \{2, \infty\}$, parameters q, n, m and a norm bound $0 < B < q$, the SIS problem w.r.t. ℓ_i-norm, denoted by $\mathsf{SIS}^{(i)}_{q,n,m,B}$, is defined as follows: given as input a matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{z} \in \mathbb{Z}_q^m$ such that $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{z}\|_i \leq B$.*

Definition 2.2. *The* LWE *problem, denoted as* $\mathsf{LWE}_{n,q,\chi}$*, where* n *is a dimension,* q *is a modulus and* χ *is a distribution over* $\mathbb{Z}$*, asks a computationally-bounded adversary* $\mathcal{A}$ *to distinguish between* $m = \mathsf{poly}(n)$ *samples drawn from either of the two distributions:*

1. $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod q)$ *for a secret* $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$*, a matrix* $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ *and an error* $\mathbf{e} \leftarrow \chi^m$*;*
2. $(\mathbf{A}, \mathbf{b})$ *for* $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ *and* $\mathbf{b} \xleftarrow{\$} \mathbb{Z}_q^m$*.*

3 Many-time Linkable Ring Signatures

3.1 Syntax

We formalize the syntax of many-time LRS. Our definitional framework is adapted from and developed based on previous works on one-time LRS [39,3]. Let T be a positive integer, a T-time linkable ring signature T-LRS is a tuple of five PPT algorithms $(\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Link})$ where:

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$: this algorithm takes as input the security parameter λ and outputs the public parameters pp. The public parameters pp includes a parameter $\mathsf{T} = \mathsf{poly}(\lambda)$.
  Without further specification, we assume that the remaining algorithms implicitly take pp as an input;
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$: on input security parameter λ, the algorithm outputs a pair of public and private keys $(\mathsf{pk}, \mathsf{sk})$;
- $\Sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, M, R)$: on input a private key sk, a message m, a list of public keys R containing the public key corresponding to sk, the algorithm outputs a signature Σ;
- $0/1 \leftarrow \mathsf{Verify}(M, R, \Sigma)$: taking as input a signature Σ, a message m, a list of public keys R, this deterministic algorithm returns a bit indicating *valid* (1) or *invalid* (0);
- $0/1 \leftarrow \mathsf{Link}\left(\{(\Sigma_i, M_i)\}_{i \in [\mathsf{T}+1]}\right)$: taking as input a set of $\mathsf{T}+1$ valid pairs of signature and message (Σ_i, M_i), this deterministic algorithm returns a bit indicating *linked* (1) or *unlinked* (0).

3.2 Security Requirements

Similar to (one-time) LRS, a T-time LRS scheme should provide *correctness*, *anonymity*, *unforgeability*, *linkability* and *non-slanderability*.

Correctness. This property requires that honestly-generated signatures are valid with overwhelming probability. Formally, given a T-LRS scheme with syntax as in Section 3.1, then for all λ, all $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$, for all $\ell \in \mathbb{N}$ and $(\mathsf{pk}_j, \mathsf{sk}_j) \leftarrow \mathsf{KeyGen}(1^\lambda)$ where $j \in [\ell]$, for all $\mathsf{pk} \in \{\mathsf{pk}_j\}_{j \in [n]}$ and for all message M, we have that

$$\mathsf{Verify}(\mathsf{Sign}(\mathsf{sk}, M, \{\mathsf{pk}_j\}_{j \in [\ell]}), M, \{\mathsf{pk}_j\}_{j \in [\ell]}) = 1 - \mathsf{negl}(\lambda),$$

where sk is the secret key associated with pk.

The definitions of anonymity, unforgeability, linkability and non-slanderability are adapted from [3,7,15]. In the experiments defining these security notions, a challenger sets up the public parameters pp and generates a set of n well-formed key pairs $\{(\mathsf{pk}_i, \mathsf{sk}_i)\}_{i\in[n]}$. It then provides an adversary with access to the following oracles:

(i) $\mathcal{CO}$: the corruption oracle $\mathcal{CO}$ takes as input an index $i \in [n]$ and returns the randomness r_i used by KeyGen for generating $(\mathsf{pk}_i, \mathsf{sk}_i)$;

(ii) $\mathcal{SO}$: the signing oracle $\mathcal{SO}$ takes as input a tuple (i, M, R) consisting of an index $i \in [n]$, a message M and a ring of public key R. If R does not contain the public key pk_i, the oracle returns a failure symbol $\perp$. Otherwise, it returns $\mathsf{Sign}(\mathsf{sk}_i, M, R)$;

We also denote by $\mathsf{I}_{\mathcal{CO}}$, $\mathsf{I}_{\mathcal{SO}}$, $\mathsf{O}_{\mathcal{SO}}$, $\mathsf{O}_{\mathcal{SO}}$ the sets recording inputs and outputs of $\mathcal{CO}$ and $\mathcal{SO}$ respectively. We remark that security is considered in the *adversarially chosen-key* model [6], where the input ring R contain malformed keys.

Anonymity. As the intended purpose of T-LRS for users to create up to T signatures without linkage, it is natural to define anonymity when an adversary can see at most T signatures from a user. We refer to this as T-*anonymity*. The experiment defining T-anonymity is as in Figure 1. An adversary can request some signatures from the targeted users with public keys $(\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1})$ before submitting the challenge message $M^\star$ and challenge ring $R^\star$. The challenger flips a random bit b and computes the challenge signature $\Sigma^\star \leftarrow \mathsf{Sign}(\mathsf{sk}_{i_b}, M, R^\star \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$. The adversary wins if it correctly guesses b, and does not request more than T signatures (including the challenge signature) from either pk_{i_0} or pk_{i_1}. We remark that, due to linking mechanism, anonymity can only be achieved if the signing secret is not exposed.

Definition 3.1. *With the syntax in Section 3.1, a* T-LRS *scheme is* T-*anonymous if for all* $\lambda \in \mathbb{N}$, *for all* $n = \mathsf{poly}(\lambda)$ *and for all PPT adversaries* $\mathcal{A}$ *in Figure 1, the advantage* $\mathsf{Adv}^{\mathsf{Tanon}}_{\mathcal{A}}(\lambda, n) := |\Pr[\mathsf{Exp}^{\mathsf{Tanon}}_{\mathcal{A}} = 1] - 1/2|$ *is negligible in* λ.

Figure 1 Experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Tanon}}$ defining T-anonymity of T-LRS

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [n]$ **do**
  $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda; r_i)$
end for
$(i_0, i_1, M^\star, R^\star, st) \leftarrow \mathcal{A}^{\mathcal{SO}}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[n]})$
$b \xleftarrow{\$} \{0,1\}$
$\Sigma^\star \leftarrow \mathcal{SO}(i_b, M^\star, R^\star \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$
$b^\star \leftarrow \mathcal{A}^{\mathcal{SO}}(\Sigma^\star, \{r_i\}_{i\in[n]\setminus\{i_0,i_1\}}, st)$
if $\#\{(i_0,\cdot,\cdot) \in \mathsf{I}_{\mathcal{CO}}\} > \mathsf{T}$ **or** $\#\{(i_1,\cdot,\cdot) \in \mathsf{I}_{\mathcal{CO}}\} > \mathsf{T}$ **then**
  return b
else
  return $b = b^\star$
end if

Unforgeability (w.r.t. insider corruption). This is identical to that of standard ring signatures. Formally, an adversary against unforgeability of T-LRS is given access to oracles $\mathcal{CO}$ and $\mathcal{SO}$ as described in (i) and (ii). It attempts to forge a signature from a ring of well-formed and uncorrupted public keys.

Definition 3.2. *With the syntax in Section 3.1, a* T-LRS *scheme is unforgeable if for all* $\lambda \in \mathbb{N}$*, for all* $n = \mathsf{poly}(\lambda)$ *and for all PPT adversaries* $\mathcal{A}$ *in Figure 2, the advantage* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{unforge}}(\lambda, n) := \Pr[\mathsf{Exp}_{\mathcal{A}}^{\mathsf{unforge}} = 1]$ *is negligible in* λ*.*

Figure 2 Experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{unforge}}$ defining unforgeability of T-LRS

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [n]$ **do**
  $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda; r_i)$
end for
$(M^\star, \Sigma^\star, R^\star) \leftarrow \mathcal{A}^{\mathcal{CO},\mathcal{SO}}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[n]})$
if $R^\star \not\subset \{\mathsf{pk}_i\}_{i\in[n]\setminus\mathcal{I}_{\mathcal{SO}}}$ **or** $(\cdot, M^\star, R^\star) \in \mathsf{I}_{\mathcal{SO}}$ **then**
  return 0
end if
return $\mathsf{Verify}(M^\star, \Sigma^\star, R^\star) = 1$

Linkability. This property requires that it is infeasible for a signer to generate $\mathsf{T}+1$ valid signatures that are unlinked. Similar to [3], we require that the event where there exists a ring of n public keys with $n\mathsf{T}+1$ valid signatures such that any subset of $\mathsf{T}+1$ signatures are unlinked, happens with negligible probability.

Definition 3.3. *With the syntax in Section 3.1, a* T-LRS *scheme is linkable if for all* $\lambda \in \mathbb{N}$*, all* $n = \mathsf{poly}(\lambda)$ *and all PPT adversaries* $\mathcal{A}$*, the advantage* $\mathsf{Adv}^{\mathsf{link}}_{\mathcal{A}}$*, defined as the following probability*

$$\Pr\left[\begin{array}{r|l} \#R = n & \\ \wedge \forall j \in [n\mathsf{T}] : \mathsf{Verify}(M^\star_j, \Sigma^\star_j, R^\star_j) = 1 & \\ \wedge \mathsf{Verify}(M^\star, \Sigma^\star, R^\star) = 1 & \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda), \\ \wedge R^\star \subset R & (\{(M^\star_j, \Sigma^\star_j, R^\star_j)\}_{j\in[n\mathsf{T}]}, \leftarrow \mathcal{A}(\mathsf{pp}), \\ \wedge \forall S \subset \mathsf{SIG}, & (M^\star, \Sigma^\star, R^\star)) \\ \#S = \mathsf{T}+1 : \mathsf{Link}(S) = 0 & \end{array}\right]$$

is negligible in λ*, wher* $R = \cup_{j\in[n\mathsf{T}]} R^\star_j$ *and* $\mathsf{SIG} = \{(\Sigma^\star_j, M^\star_j)\}_{j\in[n\mathsf{T}]} \cup \{(\Sigma^\star, M^\star)\}$.

Non-slanderability. [4] This property requires that it is infeasible to create a signature that is linked to T signatures created by an honest user. In the experiment of Figure 3, the adversary attempts to create an unseen and valid signature $\Sigma^\star$ from a ring $R^\star$ of well-formed, uncorrupted keys. It wins the game if the signature $\Sigma^\star$ can be linked to some set of T valid signatures.

Definition 3.4. *With the syntax in Section 3.1, a* T-LRS *is non-slanderable if for all* $\lambda \in \mathbb{N}$*, for all* $n = \mathsf{poly}(\lambda)$ *and all PPT adversaries* $\mathcal{A}$ *in Figure 3, the advantage* $\mathsf{Adv}^{\mathsf{sland}}_{\mathcal{A}}(\lambda, n) := \Pr[\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}(\lambda) = 1]$ *is negligible in* λ*.*

Figure 3 Experiment $\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}$ defining non-slanderability of T-LRS

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [n]$ **do**
  $(\mathsf{pk}_i, \mathsf{sk}_i)_{i\in[n]} \leftarrow \mathsf{KeyGen}(1^\lambda; r_i)$
end for
$((M^\star, \Sigma^\star, R^\star), st) \leftarrow \mathcal{A}^{\mathcal{CO},\mathcal{SO}}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[n]})$
if $R^\star \not\subset \{\mathsf{pk}_i\}_{i\in[n]\setminus \mathsf{I}_{\mathcal{CO}}}$ **or** $\mathsf{Verify}(\Sigma^\star, M^\star, R^\star) = 0$ **or** $\Sigma^\star \in \mathsf{O}_{\mathcal{SO}}$ **then**
  return 0
end if
$\{(M^\star_j, \Sigma^\star_j, R^\star_j)\}_{j\in[\mathsf{T}]} \leftarrow \mathcal{A}(\mathsf{pp}, \{r_i\}_{i\in[n]})$
if $\forall j \in [\mathsf{T}] : \mathsf{Verify}(\Sigma^\star_j, M^\star_j, R^\star_j) = 1$ **and** $\mathsf{Link}(\{(\Sigma^\star_j, M^\star_j)\}_{j\in[\mathsf{T}]} \cup \{(\Sigma^\star, M^\star)\}) = 1$ **then**
  return 1
else
  return 0
end if

[4] This is also known as *non-frameability* [3,7].

4 A Construction from Lattices

4.1 Technical Overview

Our many-time linkable ring signature can be viewed as a variant of the lattice-based ring signature from [35]. In this construction, user's public key is a binary vector $\mathbf{d} \in \{0,1\}^{n\lceil \log q \rceil}$, obtained via an SIS-based hash function from a secret $\mathbf{x} \in \{0,1\}^m$. To sign a message $M \in \{0,1\}^\star$ while hiding in a ring $R = \{\mathbf{d}_0, \ldots, \mathbf{d}_{N-1}\} \subset \{0,1\}^{n\lceil \log q \rceil}$ (here N is a power of 2), the signer uses the lattice-based accumulator from [35] (see Appendix A.3) to construct a binary tree of N leaves $\mathbf{d}_0, \ldots, \mathbf{d}_{N-1}$ with a root $\mathbf{u} \in \mathbb{Z}_q^{n\lceil \log q \rceil}$. This is done with the help of a two-input hash function

$$h_{\mathbf{A}}(\mathbf{x}_0, \mathbf{x}_1) = \mathbf{A}_0 \cdot \mathbf{x}_0 + \mathbf{A}_1 \cdot \mathbf{x}_1 \bmod q,$$

where $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{x}_0, \mathbf{x}_1 \in \{0,1\}^m$. The parent node is labeled as a hash of its two children. The signer then produces an NIZK proving that: $\mathbf{d}$ is the output of an SIS-based hash function on input $\mathbf{x}$; and $\mathbf{d}$ is a leaf in the Merkle-tree with the root $\mathbf{u}$.

To upgrade the scheme to a T-LRS scheme, we let signers include a tag $\mathbf{t}$, computed via a PRF that takes signer's secret $\mathbf{x}$ as the seed and a counter value $\mathsf{ct} \in \{0, 1, \ldots, \mathsf{T}-1\}$ as input. Note that, the pseudo-randomness of the PRF guarantees that $\mathbf{t}$ leaks little information about $\mathbf{x}$. Furthermore, any set of $\mathsf{T}+1$ signatures generated from the same secret $\mathbf{x}$ are linked, as the $\mathsf{T}+1$ tag values are computed from T inputs and therefore at least two of $\mathsf{T}+1$ tags are identical if the seed $\mathbf{x}$ is not changed.

We realize the above idea by slightly modifying the ring signature scheme from [35]: user's public key $\mathbf{d} \in \{0,1\}^{n\lceil \log q \rceil}$ is now a binary decomposition of a KTX commitment [33] to message $\mathsf{bin}(\mathbf{x})$ and randomness $\mathbf{r} \in \{0,1\}^m$, i.e.

$$\mathbf{d} = \mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}) + \mathbf{D}_1 \cdot \mathbf{r} \bmod q,$$

where $\mathbf{x} \in \mathbb{Z}_q^{m'}$. The tag $\mathbf{t}$ is computed via the BLMR lattice-based PRF [9]. Recall that, the BLMR PRF takes a uniformly random $\mathbf{k} \in \mathbb{Z}_q^{m'}$ as a seed, and on input a string $x \in \{0,1\}^\ell$ it returns the PRF value

$$\mathsf{PRF}_{\mathbf{k}}(x) = \left\lfloor \prod_{i=1}^{\ell} \mathbf{P}_{x[i]} \cdot \mathbf{k} \right\rfloor_{p,q},$$

where $\mathbf{P}_0, \mathbf{P}_1 \in \{0,1\}^{m' \times m'}$ are invertible matrices modulo q and p divides q. In our construction, the tag $\mathbf{t}$ is of the form $\mathsf{PRF}_{\mathbf{x}}(\mathsf{bin}(c))$, here $c = \mathsf{ct} \bmod \mathsf{T}$ is an integer takes value in $\{0, 1, \ldots, \mathsf{T}-1\}$. To sign a messages, signer proceeds identically as in [35], by producing an NIZK proof that $\mathbf{d}$ is accumulated in R, that $\mathbf{d}$ corresponds to a KTX commitment to $\mathbf{x}$ under randomness $\mathbf{r}$, that the tag $\mathbf{t}$ that is an output of BLMR PRF from the seed $\mathbf{x}$ and input $\mathsf{bin}(c)$.

Supporting ZK argument. In the construction, a signer needs to prove the knowledge of $(\mathbf{x}, \mathbf{r}, w, c)$ w.r.t a statement $(\mathbf{u}, \mathbf{t})$ such that:

(i) $\mathbf{d}$ is a KTX commitment to message $\mathbf{x}$ with randomness $\mathbf{r}$;
(ii) The leaf $\mathbf{d}$ is properly accumulated in $\mathbf{u}$;
(iii) T is the value of BLMR PRF evaluated on the seed $\mathbf{x}$ and input $\mathsf{bin}(c)$;
(iv) c is an integer in $\{0, 1, \ldots, \mathsf{T} - 1\}$.

To this end, we rely on the ZK argument by Yang *et al.* [61], which can handle various lattice-based relations involving quadratic constraints over the witness. Informally speaking, the statements (ii), (i), (iii) and (iv) can be transformed to certain linear equations modulo q, with some quadratic constraints over the witness. We devote Appendix C.2 for the transformations applied for each of the statements (ii), (i), (iii) and (iv). To make the argument non-interactive, we employ the generalized Unruh transformation [57,27], which can turn any special-sound, honest-verifier zero-knowledge Σ-protocol to an online-extractable and zero-knowledge NIZK argument system in QROM.

4.2 The Construction

We describe a many-time linkable ring signature scheme for rings of $N = 2^\ell = \mathsf{poly}(\lambda)$ users, that allows signer to stay completely anonymous as long as up to T signatures are issued. As discussed in Section 4.1, the scheme is an upgraded version of the ring signature from [35], where we realize linkability by the BLMR PRF [9]. Additionally, for efficiency we employ the ZK framework of [61] combining with the (generalized) Unruh transformation [57,27] to prove various relations underlying signature generation. Similar to [35], the construction can be easily adapted for the case when the ring size is not a power of 2.

Our scheme is defined by parameters $q, p, n, k, m, m', m_{\mathbf{x}}$, which are functions in the security parameter λ and the parameter l. In more details:

(I) The system modulus $q = \mathsf{poly}(\lambda)$ is used in the lattice-based components including: the KTX commitment scheme [33] (see Appendix A.2), the lattice-based accumulator of [35] (see Appendix A.3), and the BLMR lattice-based PRF [9] (see Appendix A.4). The positive integer p is chosen such that p divides q;
(II) $n = \Omega(\lambda)$ is a lattice dimensions, $k = \lceil \log q \rceil$ and $m = n\lceil \log q \rceil + \Omega(\lambda)$ is the randomness width in the KTX commitment;
(III) $m' = nk$ is the matrix dimension in the public parameters of BLMR lattice-based PRF;
(IV) Dimension $\ell_{\mathbf{x}} = m' \cdot k = n\lceil \log q \rceil^2$ specifying message dimension in the KTX commitment scheme.

To sign a message, signer needs to generate an $\mathsf{NIZKAoK}$ for the following relation:

Definition 4.1. *Define*

$$\mathcal{R}_{\mathsf{mlrs}} = \Big\{ \Big((\mathbf{A}_0, \mathbf{A}_1, \mathbf{D}_0, \mathbf{D}_1, \mathbf{P}_0, \mathbf{P}_1, \mathbf{u}, \mathbf{t}), (\mathbf{x}, \mathbf{r}, w, c) \Big) \Big\}$$

as a relation, where

- $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n \times nk}, \mathbf{D}_0 \in \mathbb{Z}_q^{n \times \ell_{\mathsf{x}}}, \mathbf{D}_1 \in \mathbb{Z}_q^{n \times m}, \mathbf{P}_0, \mathbf{P}_1 \in \{0,1\}^{m' \times m'}, \mathbf{u} \in \{0,1\}^{nk}, \mathbf{t} \in \mathbb{Z}_q^{m'}$;
- $\mathbf{x} \in \mathbb{Z}_q^{m'}, \mathbf{r} \in \{0,1\}^n, w = \big((j_1, \ldots, j_\ell) \in \{0,1\}^\ell, (\mathbf{w}_\ell, \ldots, \mathbf{w}_1) \in (\{0,1\}^{nk})^\ell\big), c \in \mathbb{N}$;
- $\mathbf{d} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(x) + \mathbf{D}_1 \cdot \mathbf{r} \bmod q)$;
- $\mathsf{TVerify}(\mathbf{u}, \mathbf{d}, w) = 1$, *i.e.* w *is a witness that* $\mathbf{d}$ *is accumulated in the root* $\mathbf{u}$, *using the lattice-based accumulator of Appendix A.3*;
- $\mathbf{t} = \Big\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c)[i]} \cdot \mathbf{x} \Big\rfloor_{p,q}$;
- $c \in \{0, 1, \ldots, \mathsf{T} - 1\}$.

By the techniques discussed in Section C.2, the relation $\mathcal{R}_{\mathsf{mlrs}}$ can be transformed into a case of the following relation

$$\{((\mathbf{A}_{\mathsf{mlrs}}, \mathbf{y}_{\mathsf{mlrs}}, \mathcal{S}_{\mathsf{mlrs}}), \mathbf{x}_{\mathsf{mlrs}}) : \mathbf{A}_{\mathsf{mlrs}} \cdot \mathbf{x}_{\mathsf{mlrs}} = \mathbf{y}_{\mathsf{mlrs}} \bmod q \\ \wedge \forall (h,i,j) \in \mathcal{S}_{\mathsf{mlrs}} : \mathbf{x}_{\mathsf{mlrs}}[h] = \mathbf{x}_{\mathsf{mlrs}}[i] \cdot \mathbf{x}_{\mathsf{mlrs}}[j] \bmod q\},$$

where $\mathbf{A}_{\mathsf{mlrs}} \in \mathbb{Z}_q^{m_{\mathsf{mlrs}} + n_{\mathsf{mlrs}}}, \mathbf{y}_{\mathsf{mlrs}} \in \mathbb{Z}_q^{m_{\mathsf{mlrs}}}$ and $\mathcal{S}_{\mathsf{mlrs}}$ is a set of 3-tuples of integers in $[n_{\mathsf{mlrs}}]$. This relation can be proven by the ZK argument system from [61]. By applying the Unruh transformation, we obtain an $\mathsf{NIZKAoK}$ for $\mathcal{R}_{\mathsf{mlrs}}$.

We now specify the algorithm of our lattice-based $\mathsf{T\text{-}LRS}$ scheme:

- $\mathsf{Setup}(1^\lambda)$: the algorithm chooses parameters as specified in (II), (III) and (IV), then does the following:
  - Choose a positive integer $\mathsf{T} = \mathsf{poly}(\lambda)$;
  - Sample $(\mathbf{D}_0, \mathbf{D}_1) \xleftarrow{\$} \mathbb{Z}_q^{n \times \ell_{\mathsf{x}}} \times \mathbb{Z}_q^{n \times m}$ as a KTX commitment key for committing to messages in the space $\{0,1\}^{\ell_{\mathsf{x}}}$;
  - Sample $(\mathbf{P}_0, \mathbf{P}_1) \xleftarrow{\$} \{0,1\}^{m' \times m'} \times \{0,1\}^{m' \times m'}$ as pubic parameters of the BLMR PRF family;
  - Sample $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times 2nk}$ that defines a function $h_{\mathbf{A}}$ from the family in Definition A.1;
  - Choose parameters defining the public key to the BDLOP commitment scheme [4], which serves as the common reference string crs to the ZK argument of [61];
  - Choose a repetition parameter $\kappa = \mathcal{O}(\lambda / \log p_0)$, here $p_0 = \mathsf{poly}(\lambda)$ is a small integer determining the soundness error $2/(2p_0 + 1)$ of the ZK argument of [61];
  - Select hash functions $\mathcal{H}_1 : \{0,1\}^* \to \{1,2,3,4\}^\kappa$, $\mathcal{H}_2 : D_{\mathsf{mlrs}} \to D_{\mathsf{mlrs}}$. Here D_{mlrs} denotes the set of all prover's responses in the underlying ZK system for $\mathcal{R}_{\mathsf{mlrs}}$. Looking forward, $\mathcal{H}_1$ and $\mathcal{H}_2$ are used in Unruh transformation to convert the ZK arguments into non-interactive versions.

Finally, output the public parameters

$$\mathsf{pp} = (q, p, n, k, m, m', \ell_{\mathbf{x}}, \mathsf{T}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{P}_0, \mathbf{P}_1, \mathbf{A}, \mathsf{crs}, \mathcal{H}_1, \mathcal{H}_2)\,.$$

– $\mathsf{KeyGen}(1^\lambda)$: the algorithm sets a counter $\mathsf{ct} = 0$, samples $\mathbf{x} \xleftarrow{\$} \mathbb{Z}_q^{m'}$ and commitment randomness $\mathbf{r} \xleftarrow{\$} \{0,1\}^m$, then computes $\mathbf{d} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}) + \mathbf{D}_1 \cdot \mathbf{r} \bmod q) \in \{0,1\}^{nk}$. Finally, it outputs $(\mathsf{pk}, \mathsf{sk}) = (\mathbf{d}, ((\mathbf{x}, \mathbf{r}), \mathsf{ct}))$.
– $\mathsf{Sign}(\mathsf{sk}, M, R)$: Given a ring $R = (\mathbf{d}_0, \ldots, \mathbf{d}_{N-1})$, where $\mathbf{d}_i \in \{0,1\}^{nk}$ for every $i \in [0, N-1]$, and $\mathsf{sk} = (\mathbf{x}, \mathbf{r}, \mathsf{ct}) \in \mathbb{Z}_q^{m'} \times \{0,1\}^m \times \mathbb{N}$ such that $\mathbf{d} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}) + \mathbf{D}_1 \cdot \mathbf{r} \bmod q) \in R$, the signer generates a ring signature Σ on $M \in \{0,1\}^*$ as follows:
  1. Compute $\mathsf{ct} \bmod \mathsf{T} = c \in \{0, 1, \ldots, \mathsf{T}-1\}$ and set $\mathsf{ct} := \mathsf{ct} + 1$. Let $\mathsf{bin}(c) \in \{0,1\}^{\lceil \log \mathsf{T} \rceil}$ be the binary representation of c, signer then computes a tag $\mathbf{t}$ from BLMR lattice-based PRF as
  $$\mathbf{t} = \mathsf{PRF}_{\mathbf{x}}(\mathsf{bin}(c)) = \left\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c)[i]} \cdot \mathbf{x} \right\rceil_{p,q} \in \mathbb{Z}_p^{m'}.$$
  2. Execute algorithm $\mathsf{TAccA}(R)$ of the accumulator scheme (see Appendix A.3) to build the Merkle tree based on R and the hash function $h_{\mathbf{A}}$, and obtain the root $\mathbf{u} \in \{0,1\}^{nk}$;
  3. Execute algorithm $\mathsf{TWitnessA}(R, \mathbf{d})$ of the accumulator scheme to obtain a witness
  $$w = \left((j_1, \ldots, j_\ell) \in \{0,1\}^\ell, (\mathbf{w}_\ell, \ldots, \mathbf{w}_1) \in (\{0,1\}^{nk})^\ell\right)$$
  that $\mathbf{d}$ is accumulated in $\mathbf{u}$;
  4. Using the witness $(\mathbf{x}, \mathbf{d}, w, c)$ generate a "signature of knowledge" (an $\mathsf{NIZKAoK}$) π_{mlrs} that $(\mathbf{u}, \mathbf{t})$ satisfies the relation $\mathcal{R}_{\mathsf{mlrs}}$ as in Definition 4.1. This is done by applying the Unruh transformation for generalized Σ-protocol [27] using hash functions $\mathcal{H}_1$ and $\mathcal{H}_2$. Specifically, when applying the transformation, it computes
  $$\mathcal{H}_1\left(\mathsf{crs}, M, \mathbf{u}, \mathbf{t}, (\mathsf{com}_i)_{[\kappa]}, (\mathsf{ch}_{i,j})_{[\kappa]\times[4]}, (h_{i,j})_{[\kappa]\times[4]}\right),$$
  where com_i, $\mathsf{ch}_{i,j}$ and $h_{i,j} = \mathcal{H}_2(\mathsf{rsp}_{\mathsf{i,j}})$ denote the commitment, challenge, hash of response generated by the prover. Let π_{mlrs} be the final proof.

  The algorithm outputs the signature $\Sigma = (\pi_{\mathsf{mlrs}}, \mathbf{t})$.

– $\mathsf{Verify}(M, R, \Sigma)$: given a message $M \in \{0,1\}^\star$, a ring $R = (\mathbf{d}_0, \ldots, \mathbf{d}_{N-1}) \subset \{0,1\}^{nk}$, and a signature $\Sigma = (\pi_{\mathsf{mlrs}}, \mathbf{t})$, this algorithm reconstructs the root $\mathbf{u} \in \{0,1\}^{nk}$ by running algorithm $\mathsf{TAccA}(R)$, then checks if the proof π_{mlrs} is a valid $\mathsf{NIZKAoK}$ for the relation $\mathcal{R}_{\mathsf{mlrs}}$. Return 1 if the check passes, otherwise return 0.

– $\mathsf{Link}(\{(\Sigma_i, M_i)\}_{i\in[\mathsf{T}+1]})$: given a set signature-message pairs $\{(\Sigma_i, M_i)\}_{i\in[\mathsf{T}+1]}$, the algorithm parses $\Sigma_i = (\pi_{\mathsf{mlrs}}^{(i)}, \mathbf{t}_i)$ and checks if among $\mathbf{t}_1, \ldots, \mathbf{t}_{\mathsf{T}+1} \in \mathbb{Z}_p^{m'}$, there exists two identical vectors. Return 1 if the check passes, otherwise return 0.

4.3 Analysis

Theorem 4.1. *The* T-LRS *scheme presented in Section 4.2 is correct.*

The above theorem is straightforward, as the correctness of our construction follows from the correctness of the lattice-based accumulator scheme of [35] and the completeness of the employed ZK argument system [61], as an honest signer always possesses a witness $(\mathbf{x}, \mathbf{r}, c, \mathbf{d})$ such that $(\mathbf{u}, \mathbf{t})$ satisfies $\mathcal{R}_{\mathsf{mlrs}}$

We analyze the efficiency of the proposed scheme regarding the asymptotic key sizes. User public key pk is a binary vector of $\{0,1\}^{nk}$ and therefore has bit length $nk = \mathcal{O}(\lambda \log \lambda)$. The corresponding secret key sk is dominated by the size of the message $\mathbf{x} \in \mathbb{Z}_q^{m'}$ and commitment randomness $\mathbf{r} \in \{0,1\}^m$. In total, the bit length of sk is $m'\lceil \log q \rceil + m = \ell_{\mathbf{x}} + m = \mathcal{O}(\lambda \log^2 \lambda)$. In particular, the key sizes only depending on the lattice dimension n and the bit-size of system modulus q.

The size of a signature Σ is dominated by the size of the NIZK proof for relations $\mathcal{R}_{\mathsf{mlrs}}$, which are $4 \cdot \kappa$ times the size of responses generated by the prover in the ZK argument [61] due to Unruh transformation. In each execution of the ZK argument of [61] for proving $\mathcal{R}_{\mathsf{mlrs}}$, the bit-size of prover's response scales linearly with lattice dimension n, logarithmically in the ring size N and logarithmically in the threshold value T. A more detailed explanation is provided at the end of Appendix C.

The security of our TS scheme is stated in the following theorem.

Theorem 4.2. *Suppose that* SIS *and* LWE *assumptions hold. Then the lattice-based* T-LRS *scheme presented in Section 4.2 is* T*-anonymous, unforgeable, linkable and non-slanderable in the QROM.*

The proof of Theorem 4.2 uses a result regarding simulation of random oracles against quantum adversary. This is crucial for zero-knowledge and online-extractability of the NIZK proof from generalized Unruh transformation.

Proposition 4.1 ([64,27]). *A uniformly random polynomial function of the degree at least $2q-1$ is perfectly indistinguishable from a random function for any PPT quantum algorithm performing at most q queries.*

We first argue anonymity of our construction.

Lemma 4.1 (T-Anonymity). *Suppose that*

- *The BLMR lattice-based PRF family is pseudorandom;*
- *The NIZK argument system for relation $\mathcal{R}_{\mathsf{mlrs}}$ is zero-knowledge.*

Then the T-LRS *scheme presented in Section 4.2 is* T*-anonymous against any PPT adversary in the QROM.*

Proof. We consider a sequence of experiments **Exp**-i. The first is the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Tanon}}$ defining T-anonymity, executed between a PPT adversary $\mathcal{A}$ and a

challenger. The last is the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Tanon}}$, modified so that the advantage of $\mathcal{A}$ is negligible. Let W_i be the probability that $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Tanon}}$ returns 1 in **Exp**-i, the advantage of $\mathcal{A}$ in **Exp**-i is then $\mathsf{Adv}_i = |\Pr[W_i] - 1/2|$.

Exp-0: This is the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{Tanon}}$ in Figure 1. The challenger sets up the public parameters and generates a ring consisting of n well-formed keys $\{(\mathsf{pk}_i, \mathsf{sk}_i)\}_{i\in[n]}$ by running $\mathsf{KeyGen}(1^\lambda; r_i)$ and gives $\{(\mathsf{pk}_i, \mathsf{sk}_i)\}_{i\in[n]}$ to an adversary $\mathcal{A}$. The adversary $\mathcal{A}$ is given accesses to the signing oracle $\mathcal{SO}$ (ii), then outputs a pair of distinct indices $(i_0, i_1) \in [n] \times [n]$ indicating the targeted public keys, a challenge message $M^\star$ and a ring $R^\star$. The challenger flips a random bit b, computes $\Sigma^\star \leftarrow \mathcal{SO}(\mathsf{sk}_{i_b}, M^\star, R^\star \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$, then provides $\mathcal{A}$ with $\Sigma^\star$ and the randomness used by KeyGen to generate the keys $\{\mathsf{pk}_i\}_{i\in[n]\setminus\{i_0,i_1\}}$. Adversary $\mathcal{A}$ can query $\mathcal{SO}$ to see signatures from either pk_{i_0} and pk_{i_1}, then it outputs a bit b' and wins if $b' = b$ and up to T signatures from either pk_{i_0} and pk_{i_1} are requested. Obviously, $\mathsf{Adv}_0 = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{Tanon}}$. We note that in **Exp**-0, adversary can query random oracles in superpositions.

Exp-1: In this experiment, we change how the challenge signature $\Sigma^\star$ is created. At the start of the experiment, the challenger chooses descriptions for $\mathcal{H}_1$, $\mathcal{H}_2$ as in Proposition 4.1. Recall that in **Exp**-1, $\Sigma^\star \leftarrow \mathcal{SO}(\mathsf{sk}_{i_b}, M^\star, R^\star \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\}$, where $\Sigma^\star = (\pi^\star_{\mathsf{mlrs}}, \mathbf{t}^\star)$. Now in **Exp**-1, the proof $\pi^\star_{\mathsf{mlrs}}$ is obtained by running the NIZK simulator, using the description of $\mathcal{H}_1$ and $\mathcal{H}_2$. The view of $\mathcal{A}$ can only changed by a negligible quantity compared to **Exp**-1 since the NIZK argument system is zero-knowledge. In particular,

$$|\mathsf{Adv}_1 - \mathsf{Adv}_0| \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{zk},\mathcal{R}_{\mathsf{mlrs}}},$$

where $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{zk},\mathcal{R}_{\mathsf{mlrs}}}$ denotes the advantage of $\mathcal{A}$ against zero-knowledge property of the NIZK argument system for relation $\mathcal{R}_{\mathsf{mlrs}}$.

Exp-2: In this experiment, we change how the challenge signature $\Sigma^\star$ is created. Recall that in **Exp**-1, $\Sigma^\star \leftarrow \mathcal{SO}(\mathsf{sk}_{i_b}, M^\star, R^\star \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$, where $\Sigma^\star = (\pi^\star_{\mathsf{mlrs}}, \mathbf{t}^\star)$, $\pi^\star_{\mathsf{mlrs}}$ is a simulated proof and $\mathbf{t}^\star$ is a PRF value computed from the seed $\mathbf{x}_{i_b} \xleftarrow{\$} \mathbb{Z}_q^m$, where $\mathsf{sk}_{i_b} = (\mathbf{x}_{i_b}, \mathbf{r}_{i_b})$. Now in **Exp**-2, the challenger samples $\mathbf{t}^\star \xleftarrow{\$} \mathbb{Z}_p^{m'}$. The view of $\mathcal{A}$ can only changed by a negligible quantity compared to **Exp**-1 since the public keys $\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}$ are statistically hiding commitments, thus revealing negligible information about $\mathbf{x}_{i_b}$. Combined with the pseudorandomness of the employed PRF (which is based on LWE assumption), it follows that $\mathcal{A}$ cannot notice the change with non-negligible probability.

We remark that adversary can only wins **Exp**-2 with probability negligibly close to $1/2$ since the signature $\Sigma^\star$ is generated independently with challenger's bit b: the proof $\pi^\star_{\mathsf{mlrs}}$ is simulated, the tag $\mathbf{t}^\star$ is a uniformly random vector. It follows that Adv_0 is negligible. □

Due to space restrictions, the proofs of unforgeability, non-slanderability and linkability are deferred to Appendix D.

References

1. Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 415–432. Springer, 2002.
2. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In Gary L. Miller, editor, *STOC 1996*, pages 99–108. ACM, 1996.
3. Michael Backes, Nico Döttling, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Ring signatures: Logarithmic-size, no setup - from standard assumptions. In *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 281–311. Springer, 2019.
4. Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In *SCN 2018*, volume 11035 of *LNCS*, pages 368–385. Springer, 2018.
5. Carsten Baum, Huang Lin, and Sabine Oechsner. Towards practical lattice-based one-time linkable ring signatures. In *ICICS 2018*, volume 11149 of *LNCS*, pages 303–322. Springer, 2018.
6. Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. *J. Cryptol.*, 22(1):114–138, 2009.
7. Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In *ASIACRYPT 2020*, volume 12492 of *LNCS*, pages 464–492. Springer, 2020.
8. Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 416–432. Springer, 2003.
9. Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan. Key homomorphic prfs and their applications. In *CRYPTO 2013*, volume 8042 of *LNCS*, pages 410–428. Springer, 2013.
10. Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *CCS 2004*, pages 168–177. ACM, 2004.
11. Jonathan Bootle, Kaoutar Elkhiyaoui, Julia Hesse, and Yacov Manevich. Dualdory: Logarithmic-verifier linkable ring signatures through preprocessing. In *ESORICS 2022*, volume 13555 of *LNCS*, pages 427–446. Springer, 2022.
12. Xavier Boyen and Thomas Haines. Forward-secure linkable ring signatures. In *ACISP 2018*, volume 10946 of *LNCS*, pages 245–264. Springer, 2018.
13. Pedro Branco and Paulo Mateus. A code-based linkable ring signature scheme. In *ProvSec 2018*, volume 11192 of *LNCS*, pages 203–219. Springer, 2018.
14. Emmanuel Bresson, Jacques Stern, and Michael Szydlo. Threshold ring signatures and applications to ad-hoc groups. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 465–480. Springer, 2002.
15. Xavier Bultel and Charles Olivier-Anclin. On the anonymity of linkable ring signatures. In *CANS 2024*, volume 14905 of *LNCS*, pages 212–235. Springer, 2024.
16. Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. In *ACM CCS 2010*, pages 201–210. ACM, 2006.
17. Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 302–321. Springer, 2005.

18. Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Balancing accountability and privacy using e-cash (extended abstract). In Roberto De Prisco and Moti Yung, editors, *SCN 2006*, volume 4116 of *LNCS*, pages 141–155. Springer, 2006.
19. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93–118. Springer, 2001.
20. David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *CRYPTO '88*, volume 403, pages 319–327. Springer, 1988.
21. David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT '91*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.
22. Wonseok Choi, Xiangyu Liu, Lirong Xia, and Vassilis Zikas. k-linkable ring signatures and applications in generalized voting. *IACR Cryptol. ePrint Arch.*, page 243, 2025.
23. Sherman S. M. Chow, Joseph K. Liu, and Duncan S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In *NDSS 2008*. The Internet Society, 2008.
24. Ivan Damgård, Kasper Dupont, and Michael Østergaard Pedersen. Unclonable group identification. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 555–572. Springer, 2006.
25. John R. Douceur. The sybil attack. In *IPTPS 2002*, volume 2429 of *LNCS*, pages 251–260. Springer, 2002.
26. Muhammed F. Esgin, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, and Dongxi Liu. Short lattice-based one-out-of-many proofs and applications to ring signatures. In *ACNS 2019*, volume 11464 of *LNCS*, pages 67–88. Springer, 2019.
27. Hanwen Feng, Jianwei Liu, and Qianhong Wu. Secure stern signatures in quantum random oracle model. In *ISC 2019*, volume 11723 of *LNCS*, pages 425–444. Springer, 2019.
28. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 1986*, volume 263 of *LNCS*, pages 186–194. Springer, 1986.
29. Dario Fiore, Lydia Garms, Dimitris Kolonelos, Claudio Soriente, and Ida Tucker. Ring signatures with user-controlled linkability. In *ESORICS 2022*, volume 13555 of *LNCS*, pages 405–426. Springer, 2022.
30. Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In *PKC 2007*, volume 4450 of *LNCS*, pages 181–200. Springer, 2007.
31. Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk. Efficient set membership proofs using mpc-in-the-head. *Proc. Priv. Enhancing Technol.*, 2022(2):304–324, 2022.
32. Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In *ICS 2010*, pages 230–240, 2010.
33. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 372–389. Springer, 2008.
34. Markulf Kohlweiss and Ian Miers. Accountable metadata-hiding escrow: A group signature case study. *Proc. Priv. Enhancing Technol.*, 2015(2):206–221, 2015.
35. Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In *EUROCRYPT 2016*, volume 9666 of *LNCS*, pages 1–31. Springer, 2016.

36. Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based prfs and applications to e-cash. In *ASIACRYPT 2017*, volume 10626 of *LNCS*, pages 304–335. Springer, 2017.
37. Benoît Libert, Khoa Nguyen, Thomas Peters, and Moti Yung. Bifurcated signatures: Folding the accountability vs. anonymity dilemma into a single private signing scheme. In *EUROCRYPT 2021*, volume 12698 of *LNCS*, pages 521–552. Springer, 2021.
38. San Ling, Khoa Nguyen, Damien Stehlé, and Huaxiong Wang. Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In *PKC 2013*, volume 7778 of *LNCS*, pages 107–124. Springer, 2013.
39. Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). In *ACISP 2004*, volume 3108 of *LNCS*, pages 325–335. Springer, 2004.
40. Zhen Liu, Khoa Nguyen, Guomin Yang, Huaxiong Wang, and Duncan S. Wong. A lattice-based linkable ring signature supporting stealth addresses. In *ESORICS 2019*, volume 11735 of *LNCS*, pages 726–746. Springer, 2019.
41. Xingye Lu, Man Ho Au, and Zhenfei Zhang. Raptor: A practical lattice-based (linkable) ring signature. In *ACNS 2019*, volume 11464 of *LNCS*, pages 110–130. Springer, 2019.
42. Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *PKC 2008*, volume 4939 of *LNCS*, pages 162–179. Springer, 2008.
43. Vadim Lyubashevsky and Ngoc Khanh Nguyen. BLOOM: bimodal lattice one-out-of-many proofs and applications. In *ASIACRYPT 2022*, volume 13794 of *LNCS*, pages 95–125. Springer, 2022.
44. Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-based signatures. In *CT-RSA 2011*, volume 6558 of *LNCS*, pages 376–392. Springer, 2011.
45. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, 2012.
46. Khoa Nguyen, Fuchun Guo, Willy Susilo, and Guomin Yang. Multimodal private signatures. In *CRYPTO 2022*, volume 13508 of *LNCS*, pages 792–822. Springer, 2022.
47. Khoa Nguyen, Partha Sarathi Roy, Willy Susilo, and Yanhong Xu. Bicameral and auditably private signatures. In *ASIACRYPT 2023*, volume 14439 of *LNCS*, pages 313–347. Springer, 2023.
48. Shen Noether. Ring signature confidential transactions for monero. *IACR Cryptol. ePrint Arch.*, page 1098, 2015.
49. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001.
50. Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Takahiro Matsuda, and Kazumasa Omote. Group signatures with message-dependent opening. In *Pairing-Based Cryptography 2012*, volume 7708 of *LNCS*, pages 270–294. Springer, 2012.
51. Hovav Shacham and Brent Waters. Efficient ring signatures without random oracles. In *PKC 2007*, volume 4450 of *LNCS*, pages 166–180. Springer, 2007.
52. Jacques Stern. A new paradigm for public key identification. *IEEE Trans. Inf. Theory*, 42(6):1757–1768, 1996.
53. Shifeng Sun, Man Ho Au, Joseph K. Liu, and Tsz Hon Yuen. Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In *ESORICS 2017*, volume 10493 of *LNCS*, pages 456–474. Springer, 2017.

54. Isamu Teranishi, Jun Furukawa, and Kazue Sako. k-times anonymous authentication (extended abstract). In *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 308–322. Springer, 2004.
55. Nam Tran, Khoa Nguyen, Dongxi Liu, Josef Pieprzyk, and Willy Susilo. Improved multimodal private signatures from lattices. In *ACISP 2024*, volume 14896 of *LNCS*, pages 3–23. Springer, 2024.
56. Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au, Joseph K. Liu, and Duncan S. Wong. Separable linkable threshold ring signatures. In *INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 384–398. Springer, 2004.
57. Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *EUROCRYPT 2015*, volume 9057 of *LNCS*, pages 755–784. Springer, 2015.
58. Shouhuai Xu and Moti Yung. Accountable ring signatures: A smart card approach. In *CARDIS 2004*, volume 153 of *IFIP*, pages 271–286. Kluwer/Springer, 2004.
59. Yuxi Xue, Xingye Lu, Man Ho Au, and Chengru Zhang. Efficient linkable ring signatures: New framework and post-quantum instantiations. In *ESORICS 2024*, volume 14985 of *LNCS*, pages 435–456. Springer, 2024.
60. Rupeng Yang, Man Ho Au, Junzuo Lai, Qiuliang Xu, and Zuoxia Yu. Lattice-based techniques for accountable anonymity: Composition of abstract stern's protocols and weak PRF with efficient protocols from LWR. *IACR Cryptol. ePrint Arch.*, page 781, 2017.
61. Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, and William Whyte. Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In *CRYPTO 2019*, volume 11692 of *LNCS*, pages 147–175. Springer, 2019.
62. Tsz Hon Yuen, Joseph K. Liu, Man Ho Au, Willy Susilo, and Jianying Zhou. Efficient linkable and/or threshold ring signature without random oracles. *Comput. J.*, 56(4):407–421, 2013.
63. Tsz Hon Yuen, Shifeng Sun, Joseph K. Liu, Man Ho Au, Muhammed F. Esgin, Qingzhao Zhang, and Dawu Gu. Ringct 3.0 for blockchain confidential transaction: Shorter size and stronger security. In *Financial Cryptography and Data Security*, volume 12059 of *LNCS*, pages 464–483. Springer, 2020.
64. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, 2012.
65. Xinyu Zhang, Joseph K. Liu, Ron Steinfeld, Veronika Kuchta, and Jiangshan Yu. Revocable and linkable ring signature. In *Inscrypt 2019*, volume 12020 of *LNCS*, pages 3–27. Springer, 2019.

A Lattice-Based Cryptographic Primitives

A.1 Discrete Gaussian and Some Statistical Results

For a full-rank lattice $\mathcal{L} \subset \mathbb{Z}^n$, a parameter $\sigma > 0$ and a vector $\mathbf{c} \in \mathbb{R}^m$, the discrete Gaussian distribution over $\mathcal{L}$ with width σ and center $\mathbf{c}$, denoted as $\mathcal{D}_{\mathcal{L},\sigma,\mathbf{c}}$ is defined such that for all $\mathbf{x} \in \mathcal{L}$ the value $\mathcal{D}_{\mathcal{L},\sigma,\mathbf{c}}(\mathbf{x})$ is proportional to $\rho_{\sigma,\mathbf{c}}(\mathbf{x})$ where $\rho_{\sigma,\mathbf{c}}$ is the Gaussian function:

$$\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(\frac{\pi \|\mathbf{x}-\mathbf{c}\|^2}{\sigma^2}\right), \forall x \in \mathbb{R}^n.$$

When the center $\mathbf{c}$ is zero, the discrete Gaussian is denoted by $\mathcal{D}_{\mathcal{L},\sigma}$. When $\mathcal{L} = \mathbb{Z}^n$, we write $\mathcal{D}_\sigma^n$ to denote the discrete Gaussian $\mathcal{D}_{\mathbb{Z}^n,\sigma}$. We stress that $\mathcal{D}_\sigma^n$ is identical to the distribution $(\mathcal{D}_{\mathbb{Z},\sigma})^n$.

We use of a variant of Leftover Hash Lemma from [32].

Lemma A.1 ([32, Lemma 1]). *Let $q \geq 2$ be an integer and $\mathcal{D}$ be a distribution over $\mathbb{Z}_q^m$ with min-entropy k. For any $\varepsilon > 0$ and $k \geq n \log q + 2\log(1/\varepsilon) + \mathcal{O}(1)$, the statistical distance between the two distributions*

$$\left\{(\mathbf{A}, \mathbf{A}\cdot\mathbf{y} \bmod q) : \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}; \mathbf{y} \leftarrow \mathcal{D}\right\},$$
$$\left\{(\mathbf{A}, \mathbf{u}) : \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}; \mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^{n}\right\}$$

is at most ε.

We also recall the notion of *gadget matrix* in [45], that is a matrix $\mathbf{G}_{n,m} \in \mathbb{Z}_q^{n\times m}$ of the form

$$\left(\mathbf{I}_n \otimes \begin{pmatrix}1 & 2 & \dots & 2^{\lceil \log q\rceil - 1}\end{pmatrix} \middle| \mathbf{0}^{m - n\lceil \log q\rceil}\right) \in \mathbb{Z}_q^{n\times m}.$$

The row vector $\mathbf{g} := \begin{pmatrix}1 & 2 & \dots & 2^{\lceil \log q\rceil - 1}\end{pmatrix}$ is called *gadget vector*.

A.2 Lattice-Based Commitment Scheme

We recall the KTX commitment scheme [33]. The commitment scheme works with a prime modulus $q = \mathsf{poly}(\lambda)$; parameters $n, m, \ell_{\mathbf{x}} \in \mathsf{poly}(\lambda)$ specifying dimensions of commitment, randomness and messages and a norm bound B on the committed message. The algorithm of the commitment scheme are as follows:

- $\mathsf{Setup}(1^\lambda)$: on input security parameter λ, choose a prime modulus $q = \mathsf{poly}(\lambda)$, choose dimensions $n, m, \ell_{\mathbf{x}} \in \mathsf{poly}(\lambda)$ such that $m = n\lceil \log q\rceil + \Omega(\lambda)$; and choose a norm bound $B = \mathsf{poly}(\lambda)$. Sample $(\mathbf{D}_0, \mathbf{D}_1) \xleftarrow{\$} \mathbb{Z}_q^{n\times \ell_{\mathbf{x}}} \times \mathbb{Z}_q^{n\times m}$ and output public parameters $\mathsf{pp} = (q, n, \ell_{\mathbf{x}}, m, B, (\mathbf{D}_0, \mathbf{D}_1))$.
- $\mathsf{Commit}(\mathbf{x})$: on input a message $\mathbf{x} \in \mathbb{Z}^{\ell_{\mathbf{x}}}$ such that $\|\mathbf{x}\|_\infty \leq B$, sample randomness $\mathbf{r} \xleftarrow{\$} \{0,1\}^m$ and output commitment $\mathbf{c} = \mathbf{D}_0\mathbf{x} + \mathbf{D}_1\mathbf{r} \bmod q$.
- $\mathsf{Open}(\mathbf{c}, (\mathbf{x}, \mathbf{r}))$: on input a commitment value $\mathbf{c} \in \mathbb{Z}_q^k$ and an opening $(\mathbf{m}, \mathbf{r})$, return 1 if and only if $\|\mathbf{m}\|_\infty \leq B, \mathbf{r} \in \{0,1\}^m$ and $\mathbf{c} = \mathbf{D}_0\mathbf{x} + \mathbf{D}_1\mathbf{r} \bmod q$.

With the above description, the KTX commitment is statistically hiding since the distribution of commitments are at a distance at most $2^{-\Omega(\lambda)}$ to uniform (Lemma A.1). The binding property relies on the hardness of $\mathsf{SIS}^{(\infty)}_{q,n,m+\ell_{\mathbf{x}},\max\{2B,1\}}$. In the special case that the message space is $\{0,1\}^{\ell_{\mathbf{x}}}$ (i.e. binary messages), then binding property reduces to $\mathsf{SIS}^{(\infty)}_{q,n,m+\ell_{\mathbf{x}},1}$

A.3 Lattice-Based Accumulator

We recall the lattice-based accumulator of [35]. The accumulator is built upon a variant of Ajtai lattice-based hash function [2].

Definition A.1. *Let q be a modulus, $k = \lceil \log q \rceil$ and m, n be positive integers such that $m = 2nk$. Consider the function family $\mathcal{H} = \{h_{\mathbf{A}} : \{0,1\}^{nk} \times \{0,1\}^{nk} \to \{0,1\}^n\}$ indexed by matrices $\mathbf{A} = [\mathbf{A}_0 \mid \mathbf{A}_1] \in \mathbb{Z}_q^{n \times m}$, where $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n \times nk}$. The function $h_{\mathbf{A}}$ is defined as $h_{\mathbf{A}}(\mathbf{u}_0, \mathbf{u}_1) = \mathsf{bin}(\mathbf{A}_0 \cdot \mathbf{u}_0 + \mathbf{A}_1 \cdot \mathbf{u}_1 \bmod q)$.*

A uniformly random function from the above family is collision resistant if the $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ problem is hard.

Now we describe the tree-based accumulator of [35] constructed from the hash family from Definition A.1.

- $\mathsf{TSetup}(1^\lambda)$: given security parameter λ, this algorithm chooses a prime modulus $q = \mathsf{poly}(\lambda)$, a dimension $n = \mathcal{O}(\lambda)$ and sets $k = \lceil \log q \rceil$, $m = 2nk$. It then samples $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ that defines a function $h_{\mathbf{A}}$ of the family $\mathcal{H}$ in Definition A.1. Finally, the algorithm returns public parameters $\mathsf{pp} = (q, n, k, m, \mathbf{A})$.

- $\mathsf{TAccA}(R = \{\mathbf{d}_0 \in \{0,1\}^{nk}, \ldots, \mathbf{d}_{N-1} \in \{0,1\}^{nk}\})$. To accumulate $N = 2^\ell$ vectors $\mathbf{d}_0, \ldots, \mathbf{d}_{N-1} \in \{0,1\}^{nk}$, for $j \in [0, N-1]$, let $\mathsf{bin}(j) = (j_1, \ldots, j_\ell) \in \{0,1\}^\ell$ be the binary representation of j and let $\mathbf{d}_j = \mathbf{u}_{j_1,\ldots,j_\ell}$. The algorithm then forms a tree of depth $\ell = \log N$ based on the N leaves $\mathbf{u}_{0,0,\ldots,0}, \ldots, \mathbf{u}_{1,1,\ldots,1}$ as follows:
  1. At depth $i \in [\ell]$, the node $\mathbf{u}_{b_1,\ldots,b_i} \in \{0,1\}^{nk}$, for all $(b_1, \ldots, b_i) \in \{0,1\}^i$, is defined as $h_{\mathbf{A}}(\mathbf{u}_{b_1,\ldots,b_i,0}, \mathbf{u}_{b_1,\ldots,b_i,1})$.
  2. At depth 0: The root $\mathbf{u} \in \{0,1\}^{nk}$ is defined as $h_{\mathbf{A}}(\mathbf{u}_0, \mathbf{u}_1)$.

  The algorithm outputs the accumulator value $\mathbf{u}$.

- $\mathsf{TWitnessA}(R, \mathbf{d})$. If $\mathbf{d} \notin R$, return $\perp$. Otherwise, $\mathbf{d} = \mathbf{d}_j$ for some $j \in [0, N-1]$ with $\mathsf{bin}(j) = (j_1, \ldots, j_\ell)$. Output the witness w defined as: $w = \left((j_1, \ldots, j_\ell), (\mathbf{u}_{j_1,\ldots,j_{\ell-1},\overline{j_\ell}}, \ldots, \mathbf{u}_{j_1,\overline{j_2}}, \mathbf{u}_{\overline{j_1}})\right) \in \{0,1\}^\ell \times (\{0,1\}^{nk})^\ell$, for $\mathbf{u}_{j_1,\ldots,j_{\ell-1},\overline{j_\ell}}, \ldots, \mathbf{u}_{j_1,\overline{j_2}}, \mathbf{u}_{\overline{j_1}}$ computed by algorithm $\mathsf{TAccA}(R)$.

- $\mathsf{TVerifyA}(\mathbf{u}, \mathbf{d}, w)$. Let the given witness w be of the form

$$w = ((j_1, \ldots, j_\ell), (\mathbf{w}_\ell, \ldots, \mathbf{w}_1)) \in \{0,1\}^\ell \times (\{0,1\}^{nk})^\ell.$$

  The algorithm reconstructs the path $\mathbf{v}_\ell, \mathbf{v}_{\ell-1}, \ldots, \mathbf{v}_1, \mathbf{v}_0 \in \{0,1\}^{nk}$ by letting $\mathbf{v}_\ell := \mathbf{d}$ and computes the $\mathbf{v}_i$'s as follows

$$\mathbf{v}_i = \begin{cases} h_{\mathbf{A}}(\mathbf{v}_{i+1}, \mathbf{w}_{i+1}), & \text{if } j_{i+1} = 0; \\ h_{\mathbf{A}}(\mathbf{w}_{i+1}, \mathbf{v}_{i+1}), & \text{if } j_{i+1} = 1. \end{cases}$$

  It returns 1 if $\mathbf{v}_0 = \mathbf{u}$. Otherwise, it returns 0.

Definition A.2. *An accumulator* $(\mathsf{TSetup}, \mathsf{TAccA}, \mathsf{TWitnessA}, \mathsf{TVerifyA})$ *is secure if for all honestly generated parameter* pp*, the probability of generating a tuple* $(R, \mathbf{d}^*, w^*)$ *such that* $(\mathsf{TVerify}(\mathsf{TAccu}(R), \mathbf{d},^*, w^*) = 1) \wedge (\mathbf{d}^* \notin R)$ *is negligible for all PPT adversaries.*

The security of the above accumulator relies on the collision resistance of $h_{\mathbf{A}}$, which in turn relies on the hardness of the $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ problem.

A.4 Lattice-Based PRF

We recall the BLMR lattice-based PRF [9]. Let q, p, n, and m be integers such that $m = n\lceil \log q \rceil$ and p divides q. The public parameters of the PRF is a pair of matrices $(\mathbf{P}_0, \mathbf{P}_1) \xleftarrow{\$} \{0,1\}^{m\times m} \times \{0,1\}^{m\times m}$ such that both matrices are invertible modulo q. The seed $\mathbf{k}$ is a uniformly random vector in $\mathbb{Z}_q^m$. The PRF $\mathsf{PRF}_{\mathbf{k}}$ takes as input a bit string $x \in \{0,1\}^L$ and outputs

$$\mathsf{PRF}_{\mathbf{k}}(x) = \left\lfloor \prod_{i=1}^{\ell} \mathbf{P}_{x[i]} \cdot \mathbf{k} \right\rfloor_{p,q}.$$

The pseudorandomness of BLMR PRF relies on the hardness of $\mathsf{LWE}_{n,q,\chi}$ where χ is a discrete Gaussian with width $\alpha \cdot q$ such that $\alpha \cdot m^{\ell} \cdot p \leq 2^{-\omega(\log n)}$

B NIZK in the QROM

We recall some results regarding NIZK proofs/arguments in QROM in [27].

B.1 Sigma Protocol

A Sigma protocol Σ for a relation $\mathcal{R}$ is a tuple $\big(D_{\text{com}}, D_{\text{ch}}, D_{\text{rsp}}, P^1_\Sigma, P^2_\Sigma, V_\Sigma\big)$; in which $D_{\text{com}}, D_{\text{ch}}, D_{\text{rsp}}$ are domains of first, second and third message respectively; (P^1_Σ, P^2_Σ) are two PPT algorithms that share a shame state and together form a prover $\mathcal{P}$; V_Σ is a deterministic, PT algorithm constituting a verifier $\mathcal{V}$ and outputting a single bit. On input $(x, w) \in \mathcal{R}$ where x is a statement and w is a corresponding witness, $P^1_\Sigma(x, w) \to \mathsf{com}$, where the first message com is called *commitment* and is sent to $\mathcal{V}$. The second message is called *challenge*, denoted by ch and is uniformly chosen from D_{ch} by $\mathcal{V}$ and is sent to the $\mathcal{P}$. The final message is called *response*, sent by $\mathcal{P}$ to $\mathcal{V}$ as $\mathsf{rsp} \leftarrow P^2_\Sigma(x, w, \mathsf{com}, \mathsf{ch})$. Finally, $\mathcal{V}$ runs V_Σ on input $(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ and accepts iff V_Σ outputs 1. The tuple $(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ is called a transcript of Σ.

A sigma protocol should satisfy the following properties:

1. **Completeness:** If $\mathcal{P}$ and $\mathcal{V}$ follow the protocol with statement x as the common input and witness w as the private input to $\mathcal{P}$, such that $(x, w) \in \mathcal{R}$; then $\mathcal{V}$ accepts with overwhelming probability.

2. **(Computational) k-special soundness:** Given a positive integer $k \geq 2$ and let $(\mathsf{com}, \mathsf{ch}_1, \mathsf{rsp}_1)$, ..., $(\mathsf{com}, \mathsf{ch}_k, \mathsf{rsp}_k)$ be k valid transcripts of Σ for a statement x, produced by some quantum PT algorithm $\mathcal{A}$, where $\mathsf{ch}_1, \ldots, \mathsf{ch}_k$ are pairwise distinct. Then there exists a PPT algorithm E_Σ called *knowledge extractor*, taking k valid transcripts as input and return a witness w such that $(x, w) \in \mathcal{R}$ with overwhelming probability.
3. **Honest verifier zero-knowledge (HVZK):** There exists a PPT algorithm S_Σ, called *simulator*, such that for all PPT quantum algorithm $\mathcal{A}$ and all $(x, w) \in \mathcal{R}$, the following quantity is negligible

$$\begin{aligned}&|\Pr[b = 1 : (\mathsf{com}, \mathsf{ch}, \mathsf{rsp}) \leftarrow (\mathcal{P}(x, w) \leftrightarrow \mathcal{V}(x)), b \leftarrow \mathcal{A}(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})] - \\ &\Pr[b = 1 : (\mathsf{com}, \mathsf{ch}, \mathsf{rsp}) \leftarrow S_\Sigma(x), b \leftarrow \mathcal{A}(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})]|.\end{aligned}$$

   Here $(\mathsf{com}, \mathsf{ch}, \mathsf{rsp}) \leftarrow (\mathcal{P}(x, w) \leftrightarrow \mathcal{V}(x))$ denotes the transcript obtained by executing protocol honestly with prover $\mathcal{P}$ and verifier $\mathcal{V}$.

B.2 NIZK protocol in QROM

A non-interactive proof protocol $\Psi = (\mathcal{P}, \mathcal{V})$ for a relation $\mathcal{R}$ can be described as $(\pi \leftarrow \mathcal{P}^{\mathcal{H}}(x, w), b \leftarrow \mathcal{V}^{\mathcal{H}}(x, \pi))$. The prover $\mathcal{P}$ and the verifier $\mathcal{V}$ are PPT algorithms, $\mathcal{H}$ is a random oracle, x is the statement, w is the witness such that $(x, w) \in \mathcal{R}$ and $b \in \{0, 1\}$. Denote by R the uniform distribution of random oracles.

For a non-interactive protocol Ψ, the following should be satisfied:

1. **Completeness:** If $\mathcal{P}$ and $\mathcal{V}$ follow the protocol with statement x as the common input and witness w as the private input to $\mathcal{P}$, such that $(x, w) \in \mathcal{R}$; then $\mathcal{V}$ outputs with overwhelming probability.
2. **Zero-knowledge:** There is a pair of algorithms (S_P, S_O) (called simulator), such that for any quantum polynomial-time algorithm $\mathcal{A}$, we have that

$$\left|\Pr[b = 1 : \mathcal{H} \leftarrow R, b \leftarrow \mathcal{A}^{\mathcal{H}, \mathcal{P}}()] - \Pr[b = 1 : \mathcal{H} \leftarrow S_O, b \leftarrow A^{\mathcal{H}, S_P}()\right|$$

   is negligible, where $\mathcal{A}^{\mathcal{H}, \mathcal{P}}$ denotes the quantum PT algorithm $\mathcal{A}$ with oracle access to $\mathcal{H}$ and $\mathcal{P}$ (similar for $A^{\mathcal{H}, S_P}$).

Another property is *online-extractability*, which is a special case of *special soundness*. Roughly speaking, online-extractability captures the ability to extract a witness without rewinding a prover. In QROM, an extractor against this property is allowed to get the circuit description of random oracles, which are generated by the random oracle simulator S_O of zero-knowledge property.

Definition B.1. *Ψ is online-extractable with respect to a simulator S_O if there exist a PPT extractor $\mathcal{E}$ such that for any quantum, PT algorithm $\mathcal{A}$, the following probability*

$$\Pr[b = 1 \wedge (x, w) \notin \mathcal{R} : \mathcal{H} \leftarrow S_O, (x, \pi) \leftarrow \mathcal{A}^{\mathcal{H}}, b \leftarrow \mathcal{P}^{\mathcal{H}}(x, \pi), w \leftarrow \mathcal{E}(\mathcal{H}, x, \pi)]$$

is negligible.

Simulation-sound online-extractability is a special case of *online-extractability*, which essentially states a witness extractor succeeds with overwhelming probability, even against an adversary that adaptively gets many simulated proofs.

Definition B.2. *Ψ is simulation-sound online-extractable, if there exist a PPT extractor $\mathcal{E}$ such that for any quantum, PT algorithm $\mathcal{A}$, the following probability*

$$\begin{aligned}\Pr[b = 1 \wedge (x,\pi) \notin \mathbb{X} \wedge (x,w) \notin \mathcal{R} :\\ \mathcal{H} \leftarrow S_O, (x,\pi) \leftarrow \mathcal{A}^{\mathcal{H},S_P}, b \leftarrow \mathcal{P}^{\mathcal{H}}(x,\pi), w \leftarrow \mathcal{E}(\mathcal{H},x,\pi)]\end{aligned}$$

is negligible. Here $\mathbb{X}$ denotes the set of proofs produced by S_P.

B.3 NIZK from Generalized Unruh Transformation

Let $\Sigma = \left(D_{\text{com}}, D_{\text{ch}}, D_{\text{rsp}}, P_\Sigma^1, P_\Sigma^2, V_\Sigma\right)$ be a sigma protocol for a relation $\mathcal{R}$ with completeness, k-special soundness and HVZK properties. The generalized Unruh transformation [27] transform Σ into a non-interactive protocol Ψ between prover $\mathcal{P}$ and verifier $\mathcal{V}$ by utilizing two hash functions $\mathcal{H}_1$ and $\mathcal{H}_2$ modeled as random oracles, where $\mathcal{H}_1 : \{0,1\}^* \to \{1,2,\ldots,m\}^t$ and $\mathcal{H}_2 : D_{\text{rsp}} \to D_{\text{rsp}}$. Here t is the number of times prover $\mathcal{P}$ needs to execute P_Σ^1 and m is a positive integer such that $m > k$. The algorithms of prover $\mathcal{P}$ and verifier $\mathcal{V}$ are as follows:

Proposition B.1 ([27]). *Let Σ be a Sigma protocol that is complete, k-special soundness and HVZK. Then the non-interactive protocol Ψ derived from Σ as described in Figure 4 and Figure 5 is complete, zero-knowledge and simulation-sound online-extractable.*

To turn Ψ into a signature of knowledge on a message M, we simply include M as an input to $\mathcal{H}_1$. That is, in the prover's algorithm in Figure 4, $\mathcal{P}$ computes

$$\mathcal{H}_1\left(M, x, (\mathsf{com}_i)_{[t]}, (\mathsf{ch}_{i,j})_{[t]\times[m]}, (h_{i,j})_{[t]\times[m]}\right).$$

In the case Σ has a common reference string crs, the NIZK prover computes

$$\mathcal{H}_1\left(\mathsf{crs}, M, x, (\mathsf{com}_i)_{[t]}, (\mathsf{ch}_{i,j})_{[t]\times[m]}, (h_{i,j})_{[t]\times[m]}\right).$$

C Supporting ZK Protocol

C.1 A Lattice-Based ZK Framework for Quadratic Relations

We recall the ZK argument system from [61]. Let n, m, ℓ be positive integer. Let $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, $\mathbf{x} \in \mathbb{Z}_q^n$ and $\mathbf{y} \in \mathbb{Z}_q^m$. Let $\mathcal{S}$ be a set of tuples (h,i,j) of integers in $[1,n]$ such that $|\mathcal{S}| = \ell$. The ZK argument system from [61] is a proof-of-knowledge protocol for the relation

$$\mathcal{R} = \{((\mathbf{A},\mathbf{y},\mathcal{S}),\mathbf{x}) : \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q \wedge \forall (h,i,j) \in \mathcal{M} : \mathbf{x}[h] = \mathbf{x}[i]\mathbf{x}[j] \bmod q\}, \tag{1}$$

Figure 4 Prover's algorithm

for $i = 1, \ldots, t$ **do**
  $\mathsf{com}_i \leftarrow P^1_{\Sigma}(x, w)$
  for $j = 1, \ldots, m$ **do**
    $\mathsf{ch}_{i,j} \xleftarrow{\$} D_{\mathrm{ch}} \backslash \{\mathsf{ch}_{i,1}, \ldots, \mathsf{ch}_{i,j-1}\}$
    $\mathsf{rsp}_{i,j} \leftarrow P^2_{\Sigma}(x, w, \mathsf{com}_i, \mathsf{ch}_{i,j})$
  end for
end for
for $i = 1, \ldots, t$ **do**
  for $j = 1, \ldots, m$ **do**
    $h_{i,j} = \mathcal{H}_2(\mathsf{rsp}_{i,j})$
  end for
end for
Parse $J_1 | \cdots | J_t := \mathcal{H}_1\left(x, (\mathsf{com}_i)_{[t]}, (\mathsf{ch}_{i,j})_{[t]\times[m]}, (h_{i,j})_{[t]\times[m]}\right)$, where $J_i \in [m]$
for $i = 1, \ldots, t$ **do**
  $\mathsf{rsp}_i := \mathsf{rsp}_{i,J_i}$
end for
$\pi := \left((\mathsf{com}_i)_{[t]}, (\mathsf{ch}_{i,j})_{[t]\times[m]}, (h_{i,j})_{[t]\times[m]}, (\mathsf{rsp}_i)_{[t]}\right)$
return π

Figure 5 Verifier $\mathcal{V}$ checks the validity of a proof π on statement x.

Parse $J_1|\cdots|J_t := \mathcal{H}_1\left(x, (\mathsf{com}_i)_{[t]}, (\mathsf{ch}_{i,j})_{[t]\times[m]}, (h_{i,j})_{[t]\times[m]}\right)$, where $J_i \in [m]$
for $i = 1, \ldots, t$ **do**
    Verify that $\mathsf{ch}_{i,1}, \ldots, \mathsf{ch}_{i,t}$ pairwise distinct
end for
for $i = 1, \ldots, t$ **do**
    Verify that $V_\Sigma(x, \mathsf{com}_i, \mathsf{ch}_{i,j}, \mathsf{rsp}_i) = 1$
end for
for $i = 1, \ldots, t$ **do**
    Verify that $h_{i,J_i} = \mathcal{H}_2(\mathsf{rsp}_{i,j})$
end for
if all checks succeed **then**
    return 1
else
    return 0
end if

The basic protocol Let λ be a security parameter and AuxCom be an arbitrary secure string commitment scheme with randomness space $\{0,1\}^\kappa$. Let l_1, l_2 be positive integer polynomial in λ; $\mathbf{B}_1$ and $\mathbf{B}_2$ are two random matrices in the form

$$\mathbf{B}_1 = \left(\begin{array}{c|cc} \mathbf{I}_{l_1} & \mathbf{B}_{1,1} \\ \mathbf{0}^{n\times l_1} & \mathbf{I}_n & \mathbf{B}_{1,2} \end{array}\right), \qquad \mathbf{B}_2 = \left(\begin{array}{c|cc} \mathbf{I}_{l_1} & \mathbf{B}_{2,1} \\ \mathbf{0}^{\ell\times l_1} & \mathbf{I}_\ell & \mathbf{B}_{2,2} \end{array}\right),$$

where $\mathbf{B}_{1,1}, \mathbf{B}_{1,2}, \mathbf{B}_{2,1}, \mathbf{B}_{2,2}$ are uniformly random matrices from $\mathbb{Z}_q^{l_1\times(l_2+n)}$, $\mathbb{Z}_q^{n\times l_2}$, $\mathbb{Z}_q^{l_1\times(l_2+\ell)}$ and $\mathbb{Z}_q^{\ell\times l_2}$ respectively. Looking forward, $\mathbf{B}_1$ and $\mathbf{B}_2$ are public parameters of the BDLOP commitment scheme [4].

In addition, the system choose a small integer $p_0 = \mathrm{poly}(\lambda)$ defining the soundness error. The randomnesses for BDLOP commitment scheme are sampled from two discrete Gaussian distributions, with width $\sigma_1 \geq \sqrt{2l_2/\pi}$ and $\sigma_2 = 2 \cdot p_0 \cdot l \cdot \log l \cdot \sigma_1$, where $l = 2l_1 + 2l_2 + n + \ell$. The system modulus q is a power of a prime q_0, i.e. $q = q_0^e$ and is chosen such that $q \geq 16p_0 \cdot \max\{l_1 + l_2 + n, l_1 + l_2 + \ell\} \cdot (\sigma_2 + p_0 \cdot \sigma_1) \cdot \mathcal{O}(\sqrt{l_1})$ and q/σ_1 is a polynomial. The common reference string is defined as

$$\mathsf{crs} = (\mathsf{AuxCom}, \mathbf{B}_1, \mathbf{B}_2, \sigma_1, \sigma_2, p)\,.$$

In the following protocol, let $\mathfrak{p}(\mathbf{v},\mathbf{z}) = \min\left(1, \frac{D^l_{\sigma_2}(\mathbf{z})}{M \cdot D^l_{\sigma_2,\mathbf{v}}(\mathbf{z})}\right)$ for any vectors $\mathbf{v},\mathbf{z} \in \mathbb{Z}^l$, where $M = e^{\mathcal{O}(1/\log^2 l)}$.

Σ-protocol for relation $\mathcal{R}$

1. **Commitment:**
   - $\mathcal{P}$ samples uniformly random $\mathbf{r} \in \mathbb{Z}_q^n$, computes $\mathbf{t} \leftarrow \mathbf{A}\cdot\mathbf{r} \bmod q$;
   - $\mathcal{P}$ samples randomnesses $\mathbf{s}_1 \leftarrow \mathcal{D}_{\sigma_1}^{l_2+n+l_1}$, $\mathbf{s}_2 \leftarrow \mathcal{D}_{\sigma_2}^{l_2+n+l_1}$, $\mathbf{s}_3 \leftarrow \mathcal{D}_{\sigma_1}^{l_2+\ell+l_1}$, $\mathbf{s}_4 \leftarrow \mathcal{D}_{\sigma_2}^{l_2+\ell+l_1}$;
   - $\mathbf{c}_1 \leftarrow \mathbf{B}_1\cdot\mathbf{s}_1 + \left(\mathbf{0}^T|\mathbf{x}^T\right)^T \bmod q$, $\mathbf{c}_2 \leftarrow \mathbf{B}_1\cdot\mathbf{s}_2 + \left(\mathbf{0}^T|\mathbf{r}^T\right)^T \bmod q$;
   - Let $\mathbf{a},\mathbf{b}$ be two vectors in $\mathbb{Z}_q^\ell$;
   - For $k \in [1,\ell]$, let (h,i,j) be the k-th element of $\mathcal{S}$ and compute
   $$\mathbf{a}[k] = \mathbf{r}[h] - \mathbf{r}[i]\cdot\mathbf{r}[j] - \mathbf{r}[j]\cdot\mathbf{x}[i], \quad \mathbf{b}[k] = \mathbf{r}[i]\cdot\mathbf{r}[j];$$
   - $\mathbf{c}_3 \leftarrow \mathbf{B}_2\cdot\mathbf{s}_3 + \left(\mathbf{0}^T|\mathbf{a}^T\right)^T$, $\mathbf{c}_4 \leftarrow \mathbf{B}_2\cdot\mathbf{s}_4 + \left(\mathbf{0}^T|\mathbf{b}^T\right)^T$;
   - Samples randomness $\rho \xleftarrow{\$} \{0,1\}^\kappa$, commits
   $$\mathsf{com}_{\mathsf{aux}} \leftarrow \mathsf{AuxCom}(\mathbf{t} \mid \mathbf{c}_1 \mid \mathbf{c}_2 \mid \mathbf{c}_3 \mid \mathbf{c}_4; \rho)$$
   and sends $\mathsf{com}_{\mathsf{aux}}$ to $\mathcal{V}$.
2. **Challenge:** $\mathcal{V}$ sends a uniformly random challenge $\mathsf{ch} \in [-p,p]$ to $\mathcal{P}$.
3. **Response:** $\mathcal{P}$ computes
   $$\mathbf{z}_0 \leftarrow \mathsf{ch}\cdot\mathbf{x} + \mathbf{r}, \quad \mathbf{z}_1 \leftarrow \mathsf{ch}\cdot\mathbf{s}_1 + \mathbf{s}_2, \quad \mathbf{z}_2 \leftarrow \mathsf{ch}\cdot\mathbf{s}_3 - \mathbf{s}_4;$$
   aborts with probability $1-\mathfrak{p}\left((\mathsf{ch}\cdot\mathbf{s}_1^T|\mathsf{ch}\cdot\mathbf{s}_2^T)^T, (\mathbf{z}_1^T|\mathbf{z}_2^T)^T\right)$, and sends the response as $\mathsf{rsp} = (\mathbf{c}_1,\mathbf{c}_3,\rho,\mathbf{z}_0,\mathbf{z}_1,\mathbf{z}_2)$.

Verification: Receiving rsp, $\mathcal{V}$ parses $\mathsf{rsp} = (\mathbf{c}_1,\mathbf{c}_3,\rho,\mathbf{z}_0,\mathbf{z}_1,\mathbf{z}_2)$ and proceeds as follows:

- Let $\mathbf{d} \in \mathbb{Z}^\ell$. For $k \in [1,\ell]$, let (h,i,j) be the k-th element of $\mathcal{S}$ and set
$$\mathbf{d}[k] \leftarrow \mathsf{ch}\cdot\mathbf{z}_0[h] - \mathbf{z}_0[i]\cdot\mathbf{z}_0[j];$$
- Set
$$\mathbf{t} \leftarrow \mathbf{A}\cdot\mathbf{z}_0 - \mathsf{ch}\cdot\mathbf{y};$$
$$\mathbf{c}_2 \leftarrow \mathbf{B}_1\cdot\mathbf{z}_1 + \left(\mathbf{0}^T|\mathbf{z}_0^T\right)^T - \mathsf{ch}\cdot\mathbf{c}_1;$$
$$\mathbf{c}_4 \leftarrow \mathsf{ch}\cdot\mathbf{c}_3 - \mathbf{B}_2\cdot\mathbf{z}_2 + \left(\mathbf{0}^T|\mathbf{d}_0^T\right)^T;$$
- Verify that:
  - $\mathsf{com}_{\mathsf{aux}} = \mathsf{AuxCom}(\mathbf{t}|\mathbf{c}_1|\mathbf{c}_2|\mathbf{c}_3|\mathbf{c}_4;\rho)$;
  - $\|\mathbf{z}_1\| \le 2\sqrt{l_1+l_2+n}\cdot(\sigma_2 + p\cdot\sigma_1)$;
  - $\|\mathbf{z}_2\| \le 2\sqrt{l_1+l_2+\ell}\cdot(\sigma_2 + p\cdot\sigma_1)$.

$\mathcal{V}$ outputs 1 if and only if all the conditions hold.

In the above protocol, we incorporate the tweaks suggested in [61] to reduce the communication cost.

Proposition C.1 (Adapted from [61]). *Suppose that $p_0 < q_0/2$, then the above protocol is a ZK argument protocol for relation $\mathcal{R}$ with completeness error $1 - 1/M$, soundness error at most $2/(2p_0 + 1)$ and is computationally honest-verifier zero knowledge under the* SIS *and* LWE *assumptions. In particular, the protocol is 3-soundness: given 3 valid pairs of challenge-response with the same commitment, there is a PPT extractor for a witness of $(\mathbf{A}, \mathbf{y}, \mathcal{S})$.*

From the protocol above, we can see that prover's response has bit size at most $\kappa + (6l_1 + 2l_2 + 3n + 2\ell) \log q_0$. Since the protocol has non-negligible completeness error due to aborting, when apply the algorithm in Figure 4 one keeps repeating the protocol until all responses are generated successfully. The number repetitions can be reduced by employing rejection sampling technique.

We note that AuxCom should be a binding and hiding string commitment scheme, which can be instantiated by the KTX commitment [33].

C.2 Proving Relations Underlying the Lattice-Based Many-time Linkable Ring Signatures

We explain how to prove the relations $\mathcal{R}_{\mathsf{mlrs}}$ in Definition 4.1. Essentially, we show that each constraint defining $\mathcal{R}_{\mathsf{mlrs}}$ can be transformed to a case of (1).

Recall that

$$\mathcal{R}_{\mathsf{mlrs}} = \Big\{ \Big((\mathbf{A}_0, \mathbf{A}_1, \mathbf{D}_0, \mathbf{D}_1, \mathbf{P}_0, \mathbf{P}_1, \mathbf{u}, \mathbf{t}), (\mathbf{x}, \mathbf{r}, w, c) \Big) \Big\},$$

where

- $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n \times nk}, \mathbf{D}_0 \in \mathbb{Z}_q^{n \times \ell_{\mathbf{x}}}, \mathbf{D}_1 \in \mathbb{Z}_q^{n \times m}, \mathbf{P}_0, \mathbf{P}_1 \in \{0,1\}^{m' \times m'}, \mathbf{u} \in \{0,1\}^{nk}, \mathbf{t} \in \mathbb{Z}_q^{m'}$;
- $\mathbf{x} \in \mathbb{Z}_q^{m'}, \mathbf{r} \in \{0,1\}^n, w = \big((j_1, \ldots, j_\ell) \in \{0,1\}^\ell, (\mathbf{w}_\ell, \ldots, \mathbf{w}_1) \in (\{0,1\}^{nk})^\ell \big)$, $c \in \mathbb{N}$;

such that

(A) $\mathbf{d} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}) + \mathbf{D}_1 \cdot \mathbf{r} \bmod q)$;
(B) $\mathsf{TVerify}(\mathbf{u}, \mathbf{d}, w) = 1$, i.e. w is a witness that $\mathbf{d}$ is accumulated in the root $\mathbf{u}$, from the lattice-based accumulator of Appendix A.3;
(C) $\mathbf{t} = \Big\lfloor \prod_{i=1}^{\ell} \mathbf{P}_{\mathsf{bin}(c)[i]} \cdot \mathbf{x} \Big\rceil_{p,q}$;
(D) $c \in \{0, 1, \ldots, \mathsf{T} - 1\}$.

Transforming statement (A) We transform statement (A) to a case of quadratic relation in 1. Note that (A) is equivalent to

$$\mathbf{G}_{n,nk} \cdot \mathbf{d} - \mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}) - \mathbf{D}_1 \cdot \mathbf{r} = \mathbf{0}^n \bmod q$$
$$\mathbf{G}_{n,\ell_{\mathbf{x}}} \cdot \mathsf{bin}(\mathbf{x}) - \mathbf{x} = \mathbf{0}^n \bmod q$$

which can be rewritten as $\mathbf{A}_1 \cdot \mathbf{x}_1 = \mathbf{0}^{2n} \bmod q$, where

$$\mathbf{A}_1 = \begin{pmatrix} \mathbf{G}_{n,nk} & -\mathbf{D}_0 & -\mathbf{D}_1 & \mathbf{0}^{n\times m'} \\ \mathbf{0}^{n\times nk} & \mathbf{G}_{n,\ell_{\mathbf{x}}} & \mathbf{0}^{n\times m} & -\mathbf{I}_{m'} \end{pmatrix} \in \mathbb{Z}_q^{m_1\times n_1},$$

and $\mathbf{x}_1 = (\mathbf{d}, \mathsf{bin}(\mathbf{x}), \mathbf{r}, \mathbf{x}) \in \mathbb{Z}^{n_1}$, where $m_1 = 2n$ and $n_1 = nk + \ell_{\mathbf{x}} + m + m'$. Note that, to enforce the binary constraint over the first $nk+\ell_{\mathbf{x}}+m$ coordinates of $\mathbf{x}_1$, we apply the observation of [61] that if q is a power of a prime and $s \in \mathbb{Z}_q$, then $s \in \{0,1\}$ if and only if $s^2 = s$. Therefore, the binary constraints can be enforced by the condition that $\mathbf{x}_1[i] \cdot \mathbf{x}_1[i] = \mathbf{x}_1[i] \bmod q$, for $i \in [nk + \ell_{\mathbf{x}} + m]$. Thus, the set $\mathcal{S}_1$ enforcing the quadratic constraints on $\mathbf{x}_1$ has size $nk + \ell_{\mathbf{x}} + m$.

Transforming statement (B) Proving statement (B), in essence, is equivalent to proving knowledge of $\mathbf{d}$ and w such that w is a witness that $\mathbf{d}$ is correctly accumulated in $\mathbf{u}$. The transformation of statement was presented in [61]. Overall, in the final matrix-vector equations $\mathbf{A}_1 \cdot \mathbf{x}_2 = \mathbf{y}_2 \bmod q$ that captures statement (B), the matrix $\mathbf{A}_2 \in \mathbb{Z}_q^{m_2\times n_2}$ and $\mathbf{x}_2 \in \mathbb{Z}^{n_2}$, where $m_2 = \ell+3n\ell$, $n_2 = 2\ell+4n\ell+2nk\ell$ and the size of the set enforcing the quadratic constraint on $\mathbf{x}_2$ is $\ell+2n\ell+2nk\ell$.

Transforming statement (C) To prove statement (C), we rewrite it as

$$\prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c)[i]} \cdot \mathbf{x} = \mathbf{v} \bmod q, \tag{2}$$

$$\lfloor p/q \cdot \mathbf{v} \rfloor = \mathbf{t} \bmod p. \tag{3}$$

Let $\ell_{\mathsf{T}} = \lceil \log \mathsf{T} \rceil$, then equation (2) can be transformed to a set of ℓ_{T} equations as follows

$$\begin{aligned} \mathbf{P}_0 \cdot (1 - \mathsf{bin}(c)[1]) \cdot \mathbf{x} + \mathbf{P}_1(\mathsf{bin}(c)[1]) \cdot \mathbf{x} &= \mathbf{v}_1 \bmod q, \\ \mathbf{P}_0 \cdot (1 - \mathsf{bin}(c)[2]) \cdot \mathbf{v}_1 + \mathbf{P}_1(\mathsf{bin}(c)[2]) \cdot \mathbf{v}_1 &= \mathbf{v}_2 \bmod q, \\ &\vdots \\ \mathbf{P}_0 \cdot (1 - \mathsf{bin}(c)[\ell_{\mathsf{T}}]) \cdot \mathbf{v}_{\ell_{\mathsf{T}}-1} + \mathbf{P}_1(\mathsf{bin}(c)[\ell_{\mathsf{T}}]) \cdot \mathbf{v}_{\ell_{\mathsf{T}}} &= \mathbf{v} \bmod q. \end{aligned}$$

Equivalently,

$$\begin{aligned} \mathbf{P}_0 \cdot \mathbf{x} + (\mathbf{P}_1 - \mathbf{P}_0) \cdot \mathsf{bin}(c)[1]\mathbf{x} - \mathbf{v}_1 &= \mathbf{0}^{m'} \bmod q, \\ \mathbf{P}_0 \cdot \mathbf{v}_1 + (\mathbf{P}_1 - \mathbf{P}_0) \cdot \mathsf{bin}(c)[2]\mathbf{v}_1 - \mathbf{v}_2 &= \mathbf{0}^{m'} \bmod q, \\ &\vdots \\ \mathbf{P}_0 \cdot \mathbf{v}_{\ell_{\mathsf{T}}-1} + (\mathbf{P}_1 - \mathbf{P}_0) \cdot \mathsf{bin}(c)[\ell_{\mathsf{T}}]\mathbf{v}_{\ell_{\mathsf{T}}-1} - \mathbf{v} &= \mathbf{0}^{m'} \bmod q. \end{aligned} \tag{4}$$

Thus, the ℓ_{T} equations of (4) can be transformed to a matrix-vector equation of the from $\mathbf{A}_3^{(1)} \cdot \mathbf{x}_3^{(1)} = \mathbf{0}^n \bmod q$, with the public matrix $\mathbf{A}_3^{(1)} \in \mathbb{Z}_q^{m_3^{(1)}\times n_3^{(1)}}$ and

the witness

$$\mathbf{x}_3^{(1)} = (\mathbf{x}, \mathbf{v}_1, \ldots, \mathbf{v}_{\ell_\mathsf{T}-1}, \mathbf{v}, \mathsf{bin}(c)[1]\mathbf{x}, \mathsf{bin}(c)[2]\mathbf{v}_1, \ldots, \mathsf{bin}(c)[\ell_\mathsf{T}]\mathbf{v}_{\ell_\mathsf{T}-1}, \mathsf{bin}(c)[1], \ldots, \mathsf{bin}(c)[\ell_\mathsf{T}]) \in \mathbb{Z}^{n_3^{(1)}}.$$

Here, we have that $m_3^{(1)} = m' \cdot \ell_\mathsf{T}$, and $n_3^{(1)} = (2\ell_\mathsf{T} + 1)m' + \ell_\mathsf{T}$. The set $\mathcal{S}_3^{(1)}$ enforcing the quadratic constraints on $\mathsf{bin}(c)[1]\mathbf{x}, \mathsf{bin}(c)[2]\mathbf{v}_1, \ldots, \mathsf{bin}(c)[\ell_\mathsf{T}]\mathbf{v}_{\ell_\mathsf{T}-1}$ and the binary constraints on $\mathsf{bin}(c)[1]\mathbf{x}, \mathsf{bin}(c)[2]\mathbf{v}_1, \ldots, \mathsf{bin}(c)[\ell_\mathsf{T}]\mathbf{v}_{\ell_\mathsf{T}-1}$ has size $\ell_\mathsf{T}m' + \ell_\mathsf{T}$.

It remains to transform equation (3) to a case of relation (1). Using the observation from [36,60], equation (3) holds if and only if the entries of the vector $\mathbf{e} := \mathbf{v} - q/p \cdot \mathbf{t}$ belong to the interval $[0, q/p)$. Therefore, we rely on the binary decomposition technique of [38]. Let $\gamma = q/p - 1$, $k_\gamma = \lfloor \log \gamma \rfloor + 1$, and

$$\mathbf{g} = ((\gamma + 1)/2^1 \mid \ldots \mid (\gamma + 2^{i-1})/2^i \mid \ldots \mid (\gamma + 2^{k_\gamma - 1})/2^{k_\gamma})$$

be a row vector. Let $\mathbf{G} = \mathbf{I}_{m'} \otimes \mathbf{g}$, then there exists a vector $\overline{\mathbf{e}} \in \{0,1\}^{m' \cdot k_\gamma}$ such that and it satisfies that $\mathbf{G} \cdot \overline{\mathbf{e}} = \mathbf{e} = \mathbf{v} - q/p \cdot \mathbf{t}$. Equivalently, $\mathbf{v} - \mathbf{G} \cdot \overline{\mathbf{e}} = q/p \cdot \mathbf{t}$. Therefore, to prove that $\mathbf{v} - \mathbf{G} \cdot \overline{\mathbf{e}} = q/p \cdot \mathbf{t}$ and $\overline{\mathbf{e}} \in \{0,1\}^{m' \cdot k_\gamma}$, we simply extend the matrix-vector equation $\mathbf{A}_3^{(1)} \cdot \mathbf{x}_3^{(1)} = \mathbf{0}^n \bmod q$ to a new matrix-vector equation of the form $\mathbf{A}_3 \cdot \mathbf{x}_3 = \mathbf{y}_3 \bmod q$, which also captures the linear equation $\mathbf{v} - \mathbf{G} \cdot \overline{\mathbf{e}} = q/p \cdot \mathbf{t}$. The witness $\mathbf{x}_3 = (\mathbf{x}_3^{(1)}, \overline{\mathbf{e}}) \in \mathbb{Z}^{n_3^{(1)} + m' \cdot k_\gamma}$. The set enforcing the quadratic constraints now includes the $m' \cdot k_\gamma$ equations enforcing the binary constraints on $\overline{\mathbf{e}}$, which now has the total size $\approx \ell_\mathsf{T}m' + \ell_\mathsf{T} + m' \cdot \log q/p$.

Transforming statement (D) To prove that c belongs to a range $[0, \mathsf{T})$, we prove in zero-knowledge the existence of another non-negative integer b such that $c + b = \mathsf{T} - 1$. In the case that $\mathsf{T} \ll q$, then we can prove the equation $c + b = \mathsf{T} - 1$ by proving that $\mathbf{g}_\mathsf{T} \cdot \mathsf{bin}(c) + \mathbf{g}_\mathsf{T} \cdot \mathsf{bin}(c) = \mathsf{T} - 1 \bmod q$, where $\mathbf{g}_\mathsf{T} = (1 \mid 2 \mid \cdots \mid 2^{\lceil \log \mathsf{T} \rceil - 1}$ is a gadget vector.

In the case that $\mathsf{T} > q$, statement (D) can be proven using the range proof presented in [61]. Let $\ell_\mathsf{T} = \lceil \log \mathsf{T} \rceil$, the equation $c + b = \mathsf{T} - 1$ can be transformed into a matrix equation by a "compression" technique as follows: let $r = \lfloor \log q \rfloor - 1$ and $l = \lceil \ell_\mathsf{T}/r \rceil$. We compress $\mathsf{bin}(b) \in \{0,1\}^{\ell_\mathsf{T}}$ to a column vector of $\mathbb{Z}_q^l$ by defining

$$\overline{\mathbf{b}} = \left(\overline{\mathbf{b}}[1] \;\; \overline{\mathbf{b}}[2] \ldots \;\; \overline{\mathbf{b}}[l]\right),$$

where $\overline{\mathbf{b}}[i] = \sum_{j=1}^{r} 2^{j-1} \cdot \mathsf{bin}(b)[(i-1) \cdot r + j]$ (for any index h such that $\ell_\mathsf{T} < h \leq lr$, we let $\mathsf{bin}(b)[h] = 0$). Similarly, let $\overline{\mathbf{c}}, \overline{\mathbf{d}}$ be the vectors of $\mathbb{Z}_q^l$ representing the integer $c, T-1$ using the compression technique as above. By considering addition

in base 2^k, the equation $c + b = T - 1$ can be rewritten as the following system

$$\begin{cases} \overline{\mathbf{c}}[1] + \overline{\mathbf{b}}[1] - 2^k \cdot \delta[1] = \overline{\mathbf{d}}[1]; \\ \overline{\mathbf{c}}[2] + \overline{\mathbf{b}}[2] + \delta[1] - 2^k \cdot \delta[2] = \overline{\mathbf{d}}[j], \\ \cdots \\ \overline{\mathbf{c}}[l-1] + \overline{\mathbf{b}}[l-1] + \delta[l-1] - 2^k \cdot \delta[l-2] = \overline{\mathbf{d}}[l-1], \\ \overline{\mathbf{c}}[l] + \overline{\mathbf{b}}[l] + \delta[l-1] = \overline{\mathbf{d}}[l]; \end{cases} \tag{5}$$

where $\delta \in \{0,1\}^{l-1}$ contains the carrying bits for each additions. Now let $\mathbf{g} = \begin{pmatrix} 1 & 2 & \dots & 2^{r-1} \end{pmatrix}$ be a row vector of $\mathbb{Z}_q^r$ and

$$\mathbf{G} = \mathbf{I}_l \otimes \mathbf{g} = \begin{pmatrix} \mathbf{g} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{g} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{g} \end{pmatrix} \in \mathbb{Z}_q^{l \times rl},$$

and

$$\mathbf{M} = \begin{pmatrix} -2^r & & & & \\ 1 & -2^r & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & 1 & -2^r \\ & & & & 1 \end{pmatrix} \in \mathbb{Z}_q^{l \times (l-1)}.$$

Observe that

$$\overline{\mathbf{b}}[i] = \mathbf{g} \cdot \begin{pmatrix} \mathsf{bin}(b)[(i-1)k+1] & \dots & \mathsf{bin}(b)[(i-1)k+k-1] & \mathsf{bin}(b)[(i-1)k+k], \end{pmatrix}$$

then the system (5) can be rewritten as

$$\begin{pmatrix} \mathbf{G} & \mathbf{G} & \mathbf{M} \end{pmatrix} \cdot \begin{pmatrix} \mathsf{bin}(c) \\ \mathsf{bin}(d) \\ \delta \end{pmatrix} = \mathsf{bin}(\mathsf{T} - 1). \tag{6}$$

Therefore, to prove that $c \in \{0, \dots, \mathsf{T} - 1\}$, one computes the integer d such that $c + d = \mathsf{T} - 1$, and forms the binary vector $\delta \in \{0,1\}^l$ so that (6) is satisfied. The matrix-vector equation capturing statement (D) is of the form $\mathbf{A}_4 \cdot \mathbf{x}_4 = \mathsf{bin}(\mathsf{T} - 1)$, where

$$\mathbf{A}_4 = \begin{pmatrix} \mathbf{G} & \mathbf{G} & \mathbf{M} \end{pmatrix} \in \mathbb{Z}_q^{m_4 \times n_4},$$

and $\mathbf{x}_4 = (\mathsf{bin}(c), \mathsf{bin}(d), \delta) \in \mathbb{Z}^{n_4}$. We have that $m_4 = l \approx \ell_\mathsf{T} / \log q$, and $n_4 = 2\ell_\mathsf{T} + l - 1 \approx 2\ell_\mathsf{T} + \ell_\mathsf{T} / \log q - 1$. The set enforcing the binary constraints over $\mathbf{x}_4$ has size exactly n_4.

Putting everything together. To prove relation $\mathcal{R}_{\mathsf{mlrs}}$ (Definition 4.1), each of the statements (A), (B), (C) and (D) defining $\mathcal{R}_{\mathsf{mlrs}}$ is transformed to a case of quadratic relation as in (1). Together, they are captured by a matrix-vector equation $\mathbf{A}_{\mathsf{mlrs}} \cdot \mathbf{x}_{\mathsf{mlrs}} = \mathbf{y}_{\mathsf{mlrs}} \bmod q$, where the public matrix $\mathbf{A}_{\mathsf{mlrs}} \in \mathbb{Z}_q^{m_{\mathsf{mlrs}} \times n_{\mathsf{mlrs}}}$ and the public vector $\mathbf{y} \in \mathbb{Z}_q^{m_{\mathsf{mlrs}}}$ are constructed from the public parameters and the pair $(\mathbf{u}, \mathbf{t})$ of accumulated value and tag. The witness $\mathbf{x}_{\mathsf{mlrs}}$ is constructed from the witness $(\mathbf{x}, \mathbf{r}, w, c)$. From the transformation techniques presented above, counting the total number of linear constraints we have that

$$m_{\mathsf{mlrs}} \approx 2n + \ell + 3n\ell + m'\ell_{\mathsf{T}} + m' + \ell_{\mathsf{T}}/\log q,$$

and the witness length

$$n_{\mathsf{mlrs}} \approx nk + \ell_{\mathbf{x}} + m + 2\ell + 4n\ell + 2nk\ell + (2\ell_{\mathsf{T}} + 1)m' + \ell_{\mathsf{T}} + m' \log q/p + 2\ell_{\mathsf{T}} + \ell_{\mathsf{T}}/\log q - 1,$$

and the size of the set $\mathcal{S}_{\mathsf{mlrs}}$ enforcing the quadratic constraints over $\mathbf{x}_{\mathsf{mlrs}}$ is

$$nk + \ell_{\mathbf{x}} + m + \ell + 2n\ell + 2nk\ell + \ell_{\mathsf{T}}m' + \ell_{\mathsf{T}} + m' \log q/p + 2\ell_{\mathsf{T}} + \ell_{\mathsf{T}}/\log q - 1.$$

The common reference string crs in the ZK argument system from the parameters $(n_{\mathsf{mlrs}}, m_{\mathsf{mlrs}}, \#\mathcal{S}_{\mathsf{mlrs}})$, by choosing an auxiliary string commitment schemes and public parameters of BDLOP commitment scheme [4]. To prove $\mathcal{R}_{\mathsf{mlrs}}$, signers run the ZK protocol with generalized Unruh transformations using the hash functions $\mathcal{H}_1$ and $\mathcal{H}_2$.

Regarding the total proof size, we remark that the bit-size of prover's response in a single execution of the Σ-protocol in Proposition C.1 is given by

$$\kappa + (6l_1 + 2l_2 + 3n_{\mathsf{mlrs}} + 2\#\mathcal{S}_{\mathsf{mlrs}}) \log q$$

As both n_{mlrs} and $\#\mathcal{S}_{\mathsf{mlrs}}$ depends linearly on n, linearly on $\ell = \log N$ where N is the ring size, and linearly in $\ell_{\mathsf{T}} = \lceil \log \mathsf{T} \rceil$, the signature size of our construction scales linearly in n, logarithmically in ring size and logarithmically in the threshold value T.

D Deferred Security Proofs

The proof of Theorem 4.2 is conducted via proving a sequence of lemmas. The first argues anonymity and is presented in Section 4.3.

We present the unforgeability proof. The proof relies on the following lemma.

Lemma D.1 ([42, Lemma 8]). *For a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *and* $\mathbf{r} \xleftarrow{\$} \{0,1\}^m$*, we have that* $\Pr[\exists \mathbf{r}' \in \{0,1\}^m \backslash \mathbf{r} : \mathbf{Ar} = \mathbf{Ar}'] \geq 1 - 2^{n \log q - m}$.

Lemma D.2 (Unforgeability). *Suppose that*

- *The NIZK argument system for relation* $\mathcal{R}_{\mathsf{mlrs}}$ *is online-extractable;*
- *The* $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ *and* $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ *problems are hard.*

Then the T-LRS *scheme presented in Section 4.2 is unforgeable against any PPT adversary in the QROM.*

Proof. Consider the experiment $\mathsf{Exp}^{\mathsf{unforge}}_{\mathcal{A}}(\lambda, n)$ of Figure 2. A challenger $\mathcal{C}$ sets up the public parameters. Then for $i \in [n]$, $\mathcal{C}$ generates n well-formed keys, by sampling $\mathbf{x}_i \xleftarrow{\$} \mathbb{Z}_q^{m'}, \mathbf{r}_i \xleftarrow{\$} \{0,1\}^m$, computing $\mathsf{pk}_i = \mathbf{d}_i = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}_i) + \mathbf{D}_1\mathbf{r}_i \bmod q)$ and sets $\mathsf{sk}_i = (\mathbf{x}_i, \mathbf{r}_i, \mathsf{ct}_i := 0\}$. Challenger $\mathcal{C}$ gives the adversary $\mathcal{A}$ the public keys $\{\mathsf{pk}_i\}_{i\in[n]}$ and provides $\mathcal{A}$ with accesses to oracles $\mathcal{CO}$ (i) and $\mathcal{SO}$ (ii). Additionally, it programs the random oracles $\mathcal{H}_1$, $\mathcal{H}_2$ by Proposition 4.1. Since the simulation can be done perfectly, the view of any PPT adversary $\mathcal{A}$ remains unchanged.

Whenever $\mathcal{A}$ outputs a forgery $(M^\star, \Sigma^\star, R^\star)$, the challenger $\mathcal{C}$ parses $\Sigma^\star = (\pi^\star_{\mathsf{mlrs}}, \mathbf{t}^\star)$ and reconstructs the accumulated value $\mathbf{u}^\star \in \{0,1\}^{nk}$ by executing $\mathsf{TAccA}(R^\star)$. It then invokes the NIZK extractor on $\pi^\star_{\mathsf{mlrs}}$ and statement $(\mathbf{u}^\star, \mathbf{t}^\star)$, using the descriptions of $\mathcal{H}_1$, $\mathcal{H}_2$. Let $(\mathbf{x}^\star, \mathbf{r}^\star, w^\star, c^\star)$ be the extracted witness. As the NIZK system is online-extractable in QROM, with overwhelming probability $(\mathbf{x}^\star, \mathbf{r}^\star, w^\star, c^\star)$ is a witness that $(\mathbf{u}^\star, \mathbf{t}^\star)$ satisfies $\mathcal{R}_{\mathsf{mlrs}}$ (Definition 4.1). In particular:

- $\mathbf{x}^\star \in \mathbb{Z}_q^{m'}$, $\mathbf{r}^\star \in \{0,1\}^m$;
- $\mathbf{d}^\star = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star) + \mathbf{D}_1 \cdot \mathbf{r}^\star \bmod q)$;
- $w^\star = \big((j_1^\star, \ldots, j_\ell^\star) \in \{0,1\}^\ell, (\mathbf{w}_\ell^\star, \ldots, \mathbf{w}_1^\star) \in (\{0,1\}^{nk})^\ell\big)$;
- $\mathsf{TVerify}(\mathbf{u}^\star, \mathbf{d}^\star, w^\star) = 1$;
- $c^\star \in \{0, 1, \ldots, \mathsf{T} - 1\}$;
- $\mathbf{t}^\star = \left\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c^\star)[i]} \cdot \mathbf{x}^\star \right\rfloor_{p,q}$;

We now consider the following cases:
Case 1: $\mathbf{d}^\star \notin R^\star$. In this case, the forger $\mathcal{A}$ breaks the security of the lattice-based accumulator, which relies on the hardness of $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$.
Case 1: $\mathbf{d}^\star \in R^\star$. In this case, note that as the ring $R^\star$ consists of well-formed and uncorrupted keys, there exists some $i^\star \in [n]$ such that

$$\mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star) + \mathbf{D}_1 \cdot \mathbf{r}^\star \bmod q) = \mathbf{d}^\star = \mathbf{d}_{i^\star} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}_{i^\star}) + \mathbf{D}_1 \cdot \mathbf{r}_{i^\star} \bmod q),$$

which implies that $\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star) + \mathbf{D}_1 \cdot \mathbf{r}^\star = \mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}_{i^\star}) + \mathbf{D}_1 \cdot \mathbf{r}_{i^\star} \bmod q$. We now consider two sub-cases:

- $\mathbf{x}_{i^\star} \neq \mathbf{x}^\star$: in this case the challenger $\mathcal{C}$ finds a message $\mathbf{x}^\star \in \mathbb{Z}_q^m$ and a randomness $\mathbf{r}^\star \in \{0,1\}^m$ that together form an opening of a KTX commitment to $\mathbf{x}_{i^\star} \neq \mathbf{x}^\star$. In other words, this breaks the binding property of commitment scheme (which, in the construction, relies on the hardness of $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$).
- $\mathbf{x}_{i^\star} = \mathbf{x}^\star$: in this case we have $\mathbf{D}_1\mathbf{r}^\star = \mathbf{D}_1\mathbf{r}_{i^\star} \bmod q$. It follows that if $\mathbf{r}_{i^\star} - \mathbf{r}^\star \neq \mathbf{0}^m$, then $\mathbf{s} = \mathbf{r}_{i^\star} - \mathbf{r}^\star \in \{-1, 0, 1\}^m$ gives a solution to an $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ instance defined by $\mathbf{D}_1$. Note that from Lemma D.1, with probability $1 - 2^{n \log q - m} \geq 1 - 2^{-\Omega(\lambda)}$, there exists some $\mathbf{r}' \in \{0,1\}^m \backslash \mathbf{r}_{i^\star}$ such that $\mathbf{D}_1 \cdot \mathbf{r}' = \mathbf{D}_1 \cdot \mathbf{r}_{i^\star} \bmod q$. Furthermore, to the forger $\mathcal{A}$'s view, the only available

information related to $\mathbf{r}_{i^\star}$ is the public key $\mathbf{d}_{i^\star}$ and the signatures output from $\mathcal{SO}(i^\star, \cdot, \cdot)$, as $\mathcal{A}$ never queries corruption oracle $\mathcal{CO}$ on $i^\star$. Since $\mathbf{d}_{i^\star}$ is distributed statistically close to uniform and the NIZK argument system is computationally zero-knowledge, $\mathcal{A}$ learns little information about $\mathbf{r}_i$ and thus with probability at least $1/2 - \mathsf{negl}(\lambda)$, we have that $\mathbf{r}_i \neq \mathbf{r}^\star$.

We conclude that any PPT adversary $\mathcal{A}$ against the unforgeability of the T-LRS scheme in Section 4.2 implies either one of the following: a PPT algorithm that breaks the online-extractability of the NIZK system; a PPT algorithm that either solves $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ or $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$. □

We remark that in the above proof, the extractor relies on the fact that the ring $R^\star$ in the forgery does not contain any corrupted key. This observation will prove useful in the non-slanderability proof.

Lemma D.3 (Non-slanderability). *Suppose that*

- *The NIZK argument system for relation $\mathcal{R}_{\mathsf{mlrs}}$ is online-extractable;*
- *The $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ and $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ problems are hard.*

Then the T-LRS *scheme presented in Section 4.2 is non-slanderable.*

Proof. Consider the experiment $\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}(\lambda, n)$ of Figure 3. A challenger $\mathcal{C}$ sets up the public parameters pp and programs the random oracles $\mathcal{H}_1$, $\mathcal{H}_2$ by Proposition 4.1. Then for $i \in [n]$, $\mathcal{C}$ generates n well-formed keys, by sampling $\mathbf{x}_i \xleftarrow{\$} \mathbb{Z}_q^{m'}, \mathbf{r}_i \xleftarrow{\$} \{0,1\}^m$, computing $\mathsf{pk}_i = \mathbf{d}_i = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}_i) + \mathbf{D}_1 \mathbf{r}_i \bmod q)$ and sets $\mathsf{sk}_i = (\mathbf{x}_i, \mathbf{r}_i, \mathsf{ct}_i := 0\}$. In the first phase, challenger $\mathcal{C}$ gives the adversary $\mathcal{A}$ the public keys $\{\mathsf{pk}_i\}_{i\in[n]}$ and provides $\mathcal{A}$ with accesses to oracles $\mathcal{CO}$ (i) and $\mathcal{SO}$ (ii), as well as accesses to $\mathcal{H}_1$ and $\mathcal{H}_2$. Adversary $\mathcal{A}$ outputs $(M^\star, \Sigma^\star, R^\star)$. In the second phase, challenger $\mathcal{C}$ then provides $\mathcal{A}$ with the randomness r_i's of KeyGen for generating $(\mathsf{pk}_i, \mathsf{sk}_i)$. Finally, $\mathcal{A}$ outputs $\{(M_j^\star, \Sigma_j^\star, R_j^\star)\}_{j\in[\mathsf{T}]}$. We show that the probability $\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}(\lambda)$ returns 1 is negligible.

If $\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}(\lambda, n)$ returns 1, the ring $R^\star$ only contains well-formed and uncorrupted keys. The challenger $\mathcal{C}$ then parses $\Sigma^\star = (\pi^\star_{\mathsf{mlrs}}, \mathbf{t}^\star)$ and reconstructs the accumulated value $\mathbf{u}^\star \in \{0,1\}^{nk}$ by executing $\mathsf{TAccA}(R_j^\star)$. It then invokes the NIZK extractor on $\pi^\star_{\mathsf{mlrs}}$ and statement $(\mathbf{u}^\star, \mathbf{t}^\star)$, using the descriptions of $\mathcal{H}_1$, $\mathcal{H}_2$. Let $(\mathbf{x}^\star, \mathbf{r}^\star, w^\star, c^\star)$ be the extracted witness. As the NIZK system is online-extractable in QROM, with overwhelming probability $(\mathbf{x}^\star, \mathbf{r}^\star, w^\star, c^\star)$ is a witness that $(\mathbf{u}^\star, \mathbf{t}^\star)$ satisfies $\mathcal{R}_{\mathsf{mlrs}}$ (Definition 4.1). In particular:

- $\mathbf{x}^\star \in \mathbb{Z}_q^{m'}$, $\mathbf{r}^\star \in \{0,1\}^m$;
- $\mathbf{d}^\star = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star) + \mathbf{D}_1 \cdot \mathbf{r}^\star \bmod q)$;
- $\mathsf{TVerify}(\mathbf{u}_j^\star, \mathbf{d}^\star, w^\star) = 1$;
- $c_j^\star \in \{0, 1, \ldots, \mathsf{T} - 1\}$;
- $\mathbf{t}^\star = \left\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c^\star)[i]} \cdot \mathbf{x}^\star \right\rfloor_{p,q}$;

Using the exact argument in the unforgeability proof, the challenger $\mathcal{C}$ can extract a solution to one of the $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ and $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ problems. Therefore, if $\mathsf{Exp}^{\mathsf{sland}}_{\mathcal{A}}(\lambda, n)$ returns 1, then either $\mathcal{A}$ violates the online-extractability of the NIZK system, or $\mathcal{A}$ can be used as a subroutine to either solve $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ or $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$. □

Lemma D.4 (Linkability). *Suppose that*

- *The NIZK argument system for relation $\mathcal{R}_{\mathsf{mlrs}}$ is online-extractable;*
- *The $\mathsf{SIS}^{(\infty)}_{q,n,\ell_{\mathbf{x}}+m,1}$, $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$ and $\mathsf{SIS}^{(\infty)}_{q,n,m,1}$ problems are hard.*

Then the T-LRS *scheme presented in Section 4.2 is linkable.*

Proof. Consider the advantage $\mathsf{Adv}^{\mathsf{link}}_{\mathcal{A}}$ in Definition 3.3. A challenger $\mathcal{C}$ sets up the public parameters pp and gives pp to adversary $\mathcal{A}$. Additionally, $\mathcal{C}$ programs the random oracles $\mathcal{H}_1$, $\mathcal{H}_2$ by Proposition 4.1. Since the simulation can be done perfectly, the view of any PPT adversary $\mathcal{A}$ remains unchanged. Finally, $\mathcal{A}$ outputs $n\mathsf{T}+1$ signatures $\left(\{(M^\star_j, \Sigma^\star_j, R^\star_j)\}_{j\in[n\mathsf{T}]}, (M^\star_0, \Sigma^\star_0, R^\star_0)\right)$. We show that the advantage $\mathsf{Adv}^{\mathsf{link}}_{\mathcal{A}}$ is negligible.

Consider the event defining the probability associating with $\mathsf{Adv}^{\mathsf{link}}_{\mathcal{A}}$, then $R = \cup_{j\in[n\mathsf{T}]} R^\star_j$ consists of n public keys. For $j \in [n\mathsf{T}]$, the challenger $\mathcal{C}$ parses $\Sigma^\star_j = ({\pi^\star_{\mathsf{mlrs}}}^{(j)}, \mathbf{t}^\star_j)$ and reconstructs the accumulated value $\mathbf{u}^\star_j \in \{0,1\}^{nk}$ by executing $\mathsf{TAccA}(R^\star_j)$. It then invokes the NIZK extractor on ${\pi^\star_{\mathsf{mlrs}}}^{(j)}$ and statement $(\mathbf{u}^\star_j, \mathbf{t}^\star_j)$, using the descriptions of $\mathcal{H}_1$, $\mathcal{H}_2$. Let $\left(\mathbf{x}^\star_j, \mathbf{r}^\star_j, w^\star_j, c^\star_j\right)$ be the extracted witness. As the NIZK system is online-extractable in QROM, with overwhelming probability $\left(\mathbf{x}^\star_j, \mathbf{r}^\star_j, w^\star_j, c^\star_j\right)$ is a witness that $(\mathbf{u}^\star_j, \mathbf{t}^\star_j)$ satisfies $\mathcal{R}_{\mathsf{mlrs}}$ (Definition 4.1). In particular:

- $\mathbf{x}^\star_j \in \mathbb{Z}_q^{m'}$, $\mathbf{r}^\star_j \in \{0,1\}^m$;
- $\mathbf{d}^\star_j = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star_j) + \mathbf{D}_1 \cdot \mathbf{r}^\star_j \bmod q)$;
- $\mathsf{TVerify}(\mathbf{u}^\star_j, \mathbf{d}^\star_j, w^\star_j) = 1$;
- $c^\star_j \in \{0, 1, \ldots, \mathsf{T}-1\}$;
- $\mathbf{t}^\star_j = \left\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c^\star_j)[i]} \cdot \mathbf{x}^\star_j \right\rfloor_{p,q}$;

Note that if there exists $j \in [n\mathsf{T}]$ such that $\mathbf{d}^\star_j \notin R^\star_j$, then $\mathcal{A}$ breaks the security of the lattice-based accumulator, which relies on the hardness of $\mathsf{SIS}^{(\infty)}_{q,n,2nk,1}$. Therefore we have that $\mathbf{d}^\star_j \in R^\star_j, \forall j \in [n\mathsf{T}]$ and in particular $\mathbf{d}^\star_j \in R = \cup_{j\in[n\mathsf{T}]} R^\star_j$

Now for $(M^\star_0, \Sigma^\star_0, R^\star_0)$, challenger $\mathcal{C}$ parses $\Sigma^\star = ({\pi^\star_{\mathsf{mlrs}}}^{(0)}, \mathbf{t}^\star_0)$, reconstructs the accumulated value $\mathbf{u}^\star_0 = \mathsf{TAccA}(R^\star_0) \in \{0,1\}^{nk}$, and invokes the NIZK extractor again to find a witness $(\mathbf{x}^\star_0, \mathbf{r}^\star_0, w^\star_0, c^\star_0)$ satisfying:

- $\mathbf{x}^\star_0 \in \mathbb{Z}_q^{m'}$, $\mathbf{r}^\star_0 \in \{0,1\}^m$;
- $\mathbf{d}^\star_0 = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}^\star_0) + \mathbf{D}_1 \cdot \mathbf{r}^\star_0 \bmod q)$;
- $\mathsf{TVerify}(\mathbf{u}^\star_0, \mathbf{d}^\star_0, w^\star_0) = 1$;
- $c^\star_0 \in \{0, 1, \ldots, \mathsf{T}-1\}$;

– $\mathbf{t}_0^\star = \left\lfloor \prod_{i=1}^{\lceil \log \mathsf{T} \rceil} \mathbf{P}_{\mathsf{bin}(c_0^\star)[i]} \cdot \mathbf{x}_0^\star \right\rfloor_{p,q}$;

Using the same argument, it must be the case that $\mathbf{d}_0^\star \in R_0^\star \subset R$. Now assume that there exist two distinct indices $j, j' \in \{0, 1, \ldots, n\mathsf{T}\}$ such that $\mathbf{d}_j^\star = \mathbf{d}_{j'}^\star = \mathbf{d} \in R$ and $\mathbf{x}_j^\star \neq \mathbf{x}_{j'}^\star$. Then $\mathbf{d}$ corresponds to a KTX commitment that opens to both $\mathbf{x}_j^\star$ and $\mathbf{x}_{j'}^\star$. This breaks the binding property of the commitment scheme. Therefore, each $\mathbf{d}_j^\star$ opens to exactly one message in the set $\{\mathbf{x}_j^\star\}_{j \in \{0,1,\ldots,n\mathsf{T}\}}$. Since $\mathbf{d}_j^\star \in R$, there can be at most n distinct values of $\mathbf{d}_j^\star$ and thus $\{\mathbf{x}_j^\star\}_{j \in [n\mathsf{T}]}$ is of size at most n.

Now consider the set $\{\mathbf{t}_j^\star\}_{j \in \{0,1,\ldots,n\mathsf{T}\}}$. Each $\mathbf{t}_j^\star$ is a BLMR PRF value evaluated on a seed from the set $\{\mathbf{x}_j^\star\}_{j \in \{0,1,\ldots,n\mathsf{T}\}}$, and on input a bit string representing an integer in the set $\{0, 1, \ldots, \mathsf{T} - 1\}$. Since there are at most n distinct seeds and at most T distinct inputs, the set $\{\mathbf{t}_j^\star\}_{j \in [n\mathsf{T}]}$ has size at most $n\mathsf{T}$. As there are $n\mathsf{T} + 1$ tags with at most $n\mathsf{T}$ distinct values, there exist two colliding tags and therefore there is a set of $\mathsf{T} + 1$ signatures that are linked. This implies that $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{link}}$ is negligible. □

E On Linkable Anonymity

We recall the notion of linkable anonymity [3,7]. Informally, when there are some users signing more than once, then it is still infeasible to associate the signatures with the correct public key, as long as these users always stay together in some ring when issuing signatures.

The experiment defining linkable anonymity (Figure 6) is adapted from [3,7,15]. In this experiment, there is a *Left-or-Right* oracle $\mathcal{LR}_b$, defined by a bit $b \in \{0, 1\}$ and two well-formed key pairs $(\mathsf{pk}_{i_0}, \mathsf{sk}_{i_0})$, $(\mathsf{pk}_{i_1}, \mathsf{sk}_{i_1})$. It takes as input an index $i \in \{i_0, i_1\}$, a message M and a ring R of public key, then:

– If $i = i_0$, the oracle returns $\mathsf{Sign}(\mathsf{sk}_{i_b}, M, R \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$.
– If $i = i_1$, the oracle returns $\mathsf{Sign}(\mathsf{sk}_{i_{1-b}}, M, R \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$.

The bit b is flipped by the challenger. An adversary can only request signatures from $\mathcal{LR}_b$ and thus it does not know which of the targeted keys pk_{i_0}, pk_{i_1} the received signature is generated under. The goal of the adversary is guessing the "key permutation" defined by b. If the adversary wins this game with probability non-negligibly far from 1/2, then it must be the case that it can associate the signatures from $\mathcal{LR}_b$ with the correct public-key.

Figure 6 Experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}}$ defining linkable anonymity

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
for $i \in [n]$ **do**
  $(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(1^\lambda; r_i)$
end for
$(i_0, i_1, st) \leftarrow \mathcal{A}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[n]})$
$b \xleftarrow{\$} \{0,1\}$
$b^\star \leftarrow \mathcal{A}^{\mathcal{LR}_b}(\mathsf{pp}, \{r_i\}_{i\in[n]\setminus\{i_0,i_1\}}, st)$
return $b = b^\star$

Definition E.1. *With the syntax in Section 3.1, a* T-LRS *scheme is linkable-anonymous if for all* $\lambda \in \mathbb{N}$*, for all* $n = \mathsf{poly}(\lambda)$ *and for all PPT adversaries* $\mathcal{A}$ *in Figure 6, the advantage* $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{link-anon}}(\lambda, n) := |\Pr[\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}} = 1] - 1/2|$ *is negligible in* λ*.*

We remark that the notion of linkable-anonymity and T-anonymity (Definition 3.1) are not directly compatible. Particularly in the case $\mathsf{T} = 1$, it was showed in [15] that there are linkable schemes that is 1-anonymous but not linkable anonymous. Nevertheless, we show that our lattice-based construction in Section 4.2 still satisfies linkable-anonymity. The intuition is that even in the case when adversary sees more than T signatures from either pk_{i_0} or pk_{i_1}, the pseudo-randomness of the tags reveals little information about the secret keys. Since both pk_{i_0} and pk_{i_1} statistically hide sk_{i_0} and sk_{i_1}; and the NIZK proof system is computationally zero-knowledge, the output of $\mathcal{LR}_b$ leaks little about either sk_{i_b} or $\mathsf{sk}_{i_{1-b}}$.

Lemma E.1 (Linkable-anonymity). *Suppose that*

- *The BLMR lattice-based PRF family is pseudorandom;*
- *The NIZK argument system for relation* $\mathcal{R}_{\mathsf{mlrs}}$ *(Definition 4.1) is zero-knowledge.*

Then the T-LRS *scheme presented in Section 4.2 is linkable-anonymous against any PPT adversary in the QROM.*

Proof. We consider a sequence of experiment **Exp**-i. The first is the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}}$ defining linkable-anonymity as in Figure 6. The last s the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}}$, modified so that the advantage of $\mathcal{A}$ is negligible. In addition, we let W_i be the probability that $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}}$ returns 1, the advantage of $\mathcal{A}$ in **Exp**-i is then $\mathsf{Adv}_i = |\Pr[W_i] - 1/2|$. We argue that all the experiments are indistinguishable (with some polynomial loss factor in the advantages).

Exp-0: This is the experiment $\mathsf{Exp}_{\mathcal{A}}^{\mathsf{link-anon}}$ in Figure 6. The challenger sets up the public parameters and generates a ring consisting of n well-formed keys $\{(\mathsf{pk}_i, \mathsf{sk}_i)\}_{i\in[n]}$ by running $\mathsf{KeyGen}(1^\lambda; r_i)$ and gives $\{(\mathsf{pk}_i, \mathsf{sk}_i)\}_{i\in[n]}$ to an adversary $\mathcal{A}$. The adversary $\mathcal{A}$ outputs a pair of distinct indices $(i_0, i_1) \in [n] \times [n]$ indicating the targeted public keys. The challenger then gives the randomness r_i

used by KeyGen to generate the keys $\{\mathsf{pk}_i\}_{i\in[n]\setminus\{i_0,i_1\}}$, flips a random bit b and provides $\mathcal{A}$ with access to the Left-or-Right oracle $\mathcal{LR}_b$. Finally, $\mathcal{A}$ outputs a bit b' and wins if $b' = b$. Obviously, $\mathsf{Adv}_0 = \mathsf{Adv}_{\mathcal{A}}^{\mathsf{link-anon}}$. We note that in **Exp**-0, adversary can query random oracles in superpositions. Furthermore, w.l.o.g we assume that the bit b is chosen right at the start.

Exp-1: In this experiment, the challenger samples a pair of distinct indices $(i_0^\star, i_1^\star) \xleftarrow{\$} [n] \times [n]$ at the start. When $\mathcal{A}$ outputs the pair $(i_0, i_1) \in [n] \times [n]$, challenger aborts and outputs a random bit if $(i_0^\star, i_1^\star) \neq (i_0, i_1)$. As **Exp**-1 and **Exp**-0 are identical when the guess $(i_0^\star, i_1^\star)$ is correct, it follows that

$$\mathsf{Adv}_1 = \mathsf{Adv}_0/n(n-1),$$

since the guess $(i_0^\star, i_1^\star)$ is independent of $\mathcal{A}'s$ view.

Exp-2: In this experiment, we change how the oracle $\mathcal{LR}_b$ responses to queries. At the start, the challenger chooses descriptions for $\mathcal{H}_1, \mathcal{H}_2$ as in Proposition 4.1. Recall that in **Exp**-1, $\mathcal{LR}_b$ takes as input (i, M, R) where $i \in \{i_0, i_1\}$. It returns a signature $\Sigma = (\pi_{\mathsf{mlrs}}, \mathbf{t})$, where $\Sigma = \mathsf{Sign}(\mathsf{sk}_{i_b}, M, R \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$ if $i = i_0$, and $\Sigma = \mathsf{Sign}(\mathsf{sk}_{i_{1-b}}, M, R \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$ if $i = i_1$. Now in **Exp**-1, the proof π_{mlrs} is obtained by running the NIZK simulator, using the description of $\mathcal{H}_1$ and $\mathcal{H}_2$. The view of $\mathcal{A}$ can only changed by a negligible quantity compared to **Exp**-1 since the NIZK argument system is zero-knowledge. In particular,

$$|\mathsf{Adv}_2 - \mathsf{Adv}_1| \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{zk},\mathcal{R}_{\mathsf{mlrs}}},$$

where $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{zk},\mathcal{R}_{\mathsf{mlrs}}}$ denotes the advantage of $\mathcal{A}$ against zero-knowledge property of the NIZK argument system for relation $\mathcal{R}_{\mathsf{mlrs}}$.

Exp-3: In this experiment, we change how the public key $\mathsf{pk}_{i_b^\star} = \mathbf{d}_{i_b^\star} \in \{0,1\}^{nk}$ is generated for $b \in \{0,1\}$. Let $\mathsf{sk}_{i_b^\star} = (\mathbf{x}_{i_b^\star}, \mathbf{r}_{i_b^\star}, \mathsf{ct}_{i_b^\star}) \in \mathbb{Z}_q^{m'} \times \{0,1\}^m \times \mathbb{N}$ be the secret key corresponding the $\mathsf{pk}_{i_b^\star}$. Note that in **Exp**-2, we have $\mathbf{d}_{i_b^\star} = \mathsf{bin}(\mathbf{D}_0 \cdot \mathsf{bin}(\mathbf{x}_{i_b^\star}) + \mathbf{D}_1 \cdot \mathbf{r}_{i_b^\star} \bmod q)$, i.e. $\mathbf{d}_{i_b^\star}$ is the binary decomposition of a KTX commitment to $\mathbf{x}_{i_b^\star}$. Now in **Exp**-3, the challenger generate $\mathbf{d}_{i_b^\star}$ by sampling $\mathbf{c}_b \xleftarrow{\$} \mathbb{Z}_q^n$ and computing $\mathbf{d}_{i_b^\star} = \mathsf{bin}(\mathbf{c}_b)$. Since the KTX commitment is statistically hiding in the setting of parameters, we have that

$$|\mathsf{Adv}_3 - \mathsf{Adv}_2| \leq 2^{-\Omega(\lambda)}.$$

Exp-4: In this experiment, we change how the oracle $\mathcal{LR}_b$ responses to queries. Recall that in **Exp**-3, the signature Σ returned from $\mathcal{LR}_b$ is a pair $(\pi_{\mathsf{mlrs}}, \mathbf{t})$, with the tag $\mathbf{t}$ is the output of BLMR PRF with seed $\mathbf{x}_{i_b}$ and input $\mathsf{bin}(c_{i_b}) \in \{0,1\}^{\lceil \log \mathsf{T} \rceil}$ such that $c_{i_b} = \mathsf{ct}_{i_b} \bmod \mathsf{T}$. Now in **Exp**-3, for each queries to $\mathcal{LR}_b$ the challenger computes the tag $\mathbf{t}$ as follows: at the start of the experiment, it samples independently, uniformly random $2\mathsf{T}$ tag values $\mathbf{t}_0^{(b)}, \ldots, \mathbf{t}_{\mathsf{T}-1}^{(b)} \in \mathbb{Z}_p^{m'}$ for $b \in \{0,1\}$. For $b' \in \{0,1\}$, whenever $\mathcal{A}$ submits a query $(i_{b'}, M, R)$ to $\mathcal{LR}_b$, for, it sets $\mathbf{t} = \mathbf{t}_{c_{i_{b'}}}^{(b')}$. The change to $\mathcal{LR}_b$ only affects the view of $\mathcal{A}$ negligibly due to the pseudorandomness of the BLMR lattice-based PRF family, and the fact

that the commitments $\mathsf{pk}_{i_b^\star}$ perfectly hides the seeds $\mathbf{x}_{i_b^\star}$. In particular, we have that

$$|\mathsf{Adv}_4 - \mathsf{Adv}_3| \leq \mathsf{Adv}_{\mathcal{A}}^{\mathsf{PRF}},$$

where $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{PRF}}$ denotes the advantage of $\mathcal{A}$ in distinguishing between the BLMR PRF family and a truly random function.

Finally, $\mathcal{A}$ wins **Exp**-4 (by correctly guessing b) with probability negligibly close to $1/2$, since the output of $\mathcal{LR}_b$ is generated independently of the bit b chosen by the challenger. □