Towards Practical Lattice-Based One-Time Linkable Ring Signatures

Carsten Baum[1], Huang Lin[2(✉)], and Sabine Oechsner[3]

[1] Department of Computer Science, Bar-Ilan University, Ramat Gan, Israel
carsten.baum@biu.ac.il
[2] ASTRI Security Lab, Hong Kong, China
linhuang@astri.org
[3] Department of Computer Science, Aarhus University, Aarhus, Denmark
oechsner@cs.au.dk

Abstract. Ring signatures, as introduced by Rivest, Shamir, and Tauman (Asiacrypt '01), allow to generate a signature for a message on behalf of an ad-hoc set of parties. To sign a message, only the public keys must be known and these can be generated independently. It is furthermore not possible to identify the actual signer based on the signature. Ring signatures have recently gained attention due to their applicability in the construction of practical anonymous cryptocurrencies, where they are used to secure transactions while hiding the identity of the actual spender. To be applicable in that setting, ring signatures must allow to determine when a party signed multiple transactions, which is done using a property called linkability.

This work presents a linkable ring signature scheme constructed from a lattice-based collision-resistant hash function. We follow the idea of existing schemes which are secure based on the hardness of the discrete logarithm problem, but adapt and optimize ours to the lattice setting. In comparison to other designs for (lattice-based) linkable ring signatures, our approach avoids the standard solution for achieving linkability, which involves proofs about correct evaluation of a pseudorandom function using heavy zero-knowledge machinery.

1 Introduction

Digital signatures are one of the most important concepts in the area of cryptography. They permit a party to generate a key pair (SK, PK), give PK to the public and add certain information Ω - called the signature - to a message

C. Baum—Supported by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office.

S. Oechsner—This work has been supported by the European Research Council (ERC) under the European Unions's Horizon 2020 research and innovation programme under grant agreement No. 669255 (MPCPRO). Part of work done while visiting NTT Secure Platform Laboratories.

D. Naccache et al. (Eds.): ICICS 2018, LNCS 11149, pp. 303–322, 2018.
https://doi.org/10.1007/978-3-030-01950-1_18

m. Ω is derived using the private (or signing) key SK and later allows a verifier, equipped with the public verification key PK, to attest that the signer indeed generated Ω for this specific message m. Verification is done in a way such that only a party who possesses certain secret information that only the signer has, namely the secret signing key SK, can generate a valid signature for PK.

Ring signatures, which were first suggested by Rivest, Shamir, and Tauman [40], relax the condition of having exactly one pair (SK, PK) for signing and verification to a certain extent. They allow a party among a set of N participants to sign a message on behalf of all of them. Here it is crucial that the verifier cannot identify the party that signed the message, while nobody outside of the N participants should be able to sign a message as if he was a participant himself. In comparison to group signatures, the set of parties does not need to be known ahead of time, but only when the signature is generated. Therefore, no key-generation algorithm which generates correlated randomness for all N parties needs to be involved and the rings can be set up ad-hoc[1].

For such a ring signature, each signer could issue an arbitrary number of signatures. Fujisaki and Suzuki introduced the notion of traceable ring signatures [17], where the signer signs a message with respect to a list of ring members and a public issue such as an election. There is a public procedure to determine whether two signatures come from one signer, i.e., the signer is linked if a signer signs the same message with respect to the same list of ring member and same issue twice [16]. A related idea is so-called *linkable ring signatures*, in which case the true signer will be linked when he signs two messages (different or identical) with respect to the same ring. In a more restricted version of linkable ring signatures, *one-time* linkable ring signatures, a signer is linked as soon as he reveals two signatures. This property has proven to be vital in the construction of cryptocurrencies, such as to prevent double spending attacks and to preserve the anonymity of a spender since the address or the respective secret key in the design of the anonymous cryptocurrency is supposed to be one-time [37].

1.1 Related Work

Lattice-Based Signature Schemes. The line of work on lattice-based signature schemes was, to the best of our knowledge, initiated by Goldreich et al. [19], while the first practical construction was based on NTRU [22]. A scheme that fits into this line of work is the provably secure construction due to Gentry et al., also called hash-and-sign [18]. This approach, where the signing key is a secret trapdoor which is used to sample a short lattice vector, was further developed in [9,15]. A different direction, called Fiat Shamir with Aborts, was first explored by Lyubashevsky [28,29]. Very efficient signature schemes such as Tesla [21] and Dilithium [14] have been designed within this framework.

[1] We relax this a bit and assume that there exists a CRS which is known to all parties and which allows them to derive their respective key pairs (SK, PK).

(Linkable) Ring Signature Schemes. There exists a wealth of literature on ring signature and linkable ring signature schemes such as [6,16,17,27,40] and we only list some of the relevant works here. However, the above mentioned signature schemes have a signature size that is linearly dependent on the number of users N in the ring. The Groth-Kohlweiss framework [20] is based on homomorphic commitments and provides a ring signature scheme with a logarithmic signature size. Franklin and Zhang [16] propose a general framework for linkable ring signatures. They extend the "PRF made public" paradigm by Bellare and Goldwasser [5] in order to provide linkability by combining a PRF evaluation of the secret key with a NIZK proof of correct evaluation. The smallest ring signatures to date have constant signature size and are based on accumulators. The construction by Dodis et al. [13] uses accumulators based on the strong RSA assumption, while Nguyen's [36] relies on pairing-based cryptography. There exists also a linkable version of [13] by Tsang and Wei [42] that retains the constant-sized signatures. There exist candidates for post-quantum ring signature schemes such as hash-based [12,23] or multi-variate-quadratic-equation based constructions [35]. Neither of them provide linkability in their current form, but they can potentially be extended to do so.

Lattice-Based Ring Signature Schemes. Lattice-based ring signatures were first introduced explicitly through the work of Brakerski and Tauman-Kalai [10] who proposed a general framework for ring signatures in the standard model and showed how to instantiate it based on the SIS assumption. The resulting signatures have size $O(mN)$ for message length m and ring size N. Subsequently, Wang and Sun [43] proposed two ring signatures schemes from the SIS assumption in the random oracle and standard model, respectively, both of linear signature size. The first ring signature scheme based on the LWE assumption was proposed by Melchor et al. [33] and is an extension of [28] to the ring signature setting. Like the previous schemes, it yields signatures of linear size. Recently, Libert et al. [25] proposed the first lattice-based ring signature scheme with only logarithmic signature size using a Merkle-tree based construction.

Concurrent Work. In concurrent work, Torres et al. [41] present a construction that is very similar to ours. When comparing the actual parameters of both, we have a larger size of the public keys, but compare favorably in the signature size.

1.2 Our Contribution

We present a lattice-based linkable ring signature scheme based on the Module-SIS and Module-LWE problem. Our scheme has a signature size which is linear in N. It is therefore asymptotically less efficient than e.g. [12,23,25]. However, we show that in terms of signature size our construction outperforms or performs as good as [12,25] for comparable security levels for ring sizes $N \lessapprox 128$ and beats [23] for rings of small size. A comparison can be found in Table 1 below.

Table 1. Comparison with existing work

	[25]	[12] Sponge/Davies-Meyer	[23]	Our work
Size of PK	0.5 KB	32 B	32 B	8 KB
Size ($N = 8$)	1.44 MB	766/477 KB	148 KB	82.5 KB
Size ($N = 32$)	2.29 MB	1200/719 KB	216 KB	305.7 KB
Size ($N = 128$)	3.14 MB	1.59/0.94 MB	285 KB	1.17 MB

The authors of [12] present two different, highly optimized constructions of ring signatures in their work. We mention numbers for both to allow for fair comparison (outperforming one of the two for $N = 128$). We want to stress that using known techniques [14] and by choosing parameters more aggressively it is possible to reduce the public key and signature size in our setting further, but such optimizations are beyond the scope of this work. Furthermore, [12,23,25] are not linkable in their current form, so one can expect a further increase in their proof size to compute a linkability tag. Though our work only outperforms [23] for small ($N \leq 20$) ring sizes, this is exactly the range that cryptocurrencies need: the recommended ring size of the most popular cryptocurrency using linkable ring signatures, Monero, at the time of writing was $N = 5$. As mentioned before, using [14], would make it possible to reduce the ring signature size further to also outperform [23] for $N \lessapprox 64$.

1.3 Technical Overview

As mentioned before, the standard approach for transforming a ring signature scheme into a linkable ring signature scheme, following Franklin and Zhang [16], is to add a PRF evaluation of the signer's secret key to the signature, as well as a zero-knowledge proof of correct evaluation of the PRF under one of the secret keys corresponding to the public keys. This generic approach applies to any ring signature scheme and was explored for lattice-based PRFs in [25,26,44]. However, such proofs come with quite a substantial overhead. Our construction instead follows the approach of Liu et al. [27] that avoids this technique. The main observation is that the signer in their scheme has two "public" keys: One that is published before signature generation as part of the ring of signers, and the other one that is appended to each signature. Hence, another"public key" under different public parameters that corresponds to the signer's secret signing key can be used as linkability tag. Since both kinds of public keys share the same algebraic structure, the two "public keys" of the signer, i.e. the actual public key and the linkability tag, can be tied together without appending another non-interactive zero-knowledge proof to the signature.

Since our construction will be based on the (Module-)SIS and (Module-)LWE problem, the public keys of the parties are of the form $PK = \boldsymbol{Ar}$ for secret key $\boldsymbol{r}$ and public matrix $\boldsymbol{A}$. Linkability will be ensured by providing linkability tags $I = \boldsymbol{Br}$ for another public matrix $\boldsymbol{B}$. Interestingly, the reason why our

construction achieves only one-time linkability is inherent in this approach: any evaluation $\boldsymbol{Br}$ leaks information about $\boldsymbol{r}$. If a fresh matrix $\boldsymbol{B}$ is generated for each ring, then a malicious party can receive more leakage on $\boldsymbol{r}$ than intended and hence may be able to recover the signer's secret key.

In order to obtain more efficient lattice-based (linkable) ring signatures, it may be tempting to try to instantiate current sublinear-size ring signatures in the lattice setting. Note, however, that this is far from trivial, as these solutions are specifically tailored to a certain assumption like Dodis et al.'s accumulator-based ring signatures [13], or suffer from the well-known problem that hard lattice assumptions do not provide enough algebraic structure to support existing sublinear approaches based on homomorphic operations like that of Groth and Kohlweiss [20].

Paper Organization
In Sect. 2 we will introduce some definitions and lemmas concerning lattice-based constructions which we will need throughout this work. Moreover, we will give definitions for linkable ring signatures (following previous work). Section 3 contains the construction and security statements. The main parts of the proofs are deferred to Appendix A, whereas we discuss the practicality of our scheme in Sect. 4. In this Section, we also provide a sample parameter set for our construction together with estimates for the size of signatures.

2 Preliminaries

We will use $[N]$ as shorthand for the set $\{1, \ldots, N\}$. Let R be the cyclotomic ring $R = \mathbb{Z}[X]/\langle X^\nu + 1\rangle$, where $\nu = 2^p$ and $p \in \mathbb{N}^+$. Let q be an odd prime and define $R_q = \mathbb{Z}_q[X]/\langle X^\nu + 1\rangle$. Here $\mathbb{Z}_q$ denotes the integers modulo q, which will be represented as elements from the interval $\left[-\frac{q-1}{2}, \frac{q-1}{2}\right]$. For $f = \sum_i f_i X^i \in R$, the norms of f are defined as

$$l_1 : \|f\|_1 = \sum\nolimits_i |f_i|,\ l_2 : \|f\|_2 = \left(\sum\nolimits_i |f_i|^2\right)^{1/2},\ l_\infty : \|f\|_\infty = \max_i |f_i|\,.$$

If $f \in R_q$, then we will represent each coset from $\mathbb{Z}_q$ with its unique representative from the aforementioned interval and consider the norm of the obtained $\mathbb{Z}$-vector. Let S_β denote the set of elements $x \in R$ with l_∞-norm at most β. Let $\mathbf{0}_v \in \mathbb{Z}^{v\times v}$ and $\mathbf{I}_v \in \mathbb{Z}^{v\times v}$ denote the zero and identity matrix over $\mathbb{Z}$.

Remark 1. We use the following standard relations among different l-norms of a vector in R as defined above:

1. If $f, g \in R$ such that $\|f\|_\infty \leq \beta$, $\|g\|_1 \leq \gamma$, then $\|fg\|_\infty \leq \beta\gamma$.
2. If $f \in R$, $\boldsymbol{g} \in R^v$ satisfy that $\|f\|_2 \leq \beta$, $\|\boldsymbol{g}\|_\infty \leq \gamma$, then $\|f\boldsymbol{g}\|_2 \leq \sqrt{v}\nu\beta\gamma$.

We require a subset D of R_q which consists of short invertible elements such that the difference of any two distinct elements from this set is also invertible. It was shown in [32] that as long as q is a prime that satisfies $q = 17 \mod 32$ and $q > 2^{20}$, then the set $D = \{d \in R_q | \|d\|_\infty \leq 1, \|d\|_1 \leq \kappa\}$ satisfies this requirement. We use $\bar{D}$ to denote the set of values $D + D$ excluding 0.

2.1 Normal Distribution and Rejection Sampling

The continuous normal distribution over $\mathbb{R}^\nu$ centered at $\boldsymbol{u} \in \mathbb{R}^\nu$ with standard deviation σ has probability density function

$$\rho^\nu_{\boldsymbol{u},\sigma}(\boldsymbol{x}) = \frac{1}{\sqrt{2\pi}\sigma} \cdot \exp\left(\frac{-||\boldsymbol{x}-\boldsymbol{u}||_2^2}{2\sigma^2}\right)$$

The *discrete normal distribution* over R^v centered at $\boldsymbol{u} \in R^v$ with standard deviation σ is given by the distribution function (for all $\boldsymbol{x} \in R^v$)

$$\mathcal{N}_{\boldsymbol{u},\sigma}(\boldsymbol{x}) = \rho^{v\cdot\nu}_{\boldsymbol{u},\sigma}(\boldsymbol{x}) / \rho^{v\cdot\nu}_{\sigma}(R^v),$$

where we omit the subscript $\boldsymbol{u}$ when it is zero. We use the following standard tail-bound due to Banaszczyk:

Lemma 1. *Let $\mathcal{N}_{\boldsymbol{u},\sigma}$ be defined as above. Then*

$$\Pr\left[\|\boldsymbol{z}\|_2 > 2\sigma\sqrt{v\nu} | \boldsymbol{z} \leftarrow \mathcal{N}^v_\sigma\right] < 2^{-v\nu}$$

For our ring signature scheme, we use rejection sampling to hide the secret signing key. The basic idea of rejection sampling is to abort the protocol with a certain probability such that the distribution of the response is independent of the secret input. We adopt the rejection sampling lemma from [29]:

Lemma 2. *Let V be a subset of R^v in such that all elements have $\|\cdot\|_2$-norms less than T, $\sigma \in \mathbb{R}$ such that $\sigma = \omega(T\sqrt{\log(v\nu)})$, and $h : V \to \mathbb{R}$ be a probability distribution. Then there exists an $M = O(1)$ such that the output distribution of the following two algorithms $\mathcal{A}$, $\mathcal{S}$ is within statistical distance $2^{-\omega(\log(v\nu))}/M$:*

$\mathcal{A}$**:**

1. $\boldsymbol{u} \leftarrow h$
2. $\boldsymbol{z} \leftarrow \mathcal{N}^v_{\boldsymbol{u},\sigma}$
3. *output* $(\boldsymbol{u}, \boldsymbol{z})$ *with probability* $\min\left(\frac{1}{M}\frac{\mathcal{N}^v_\sigma(\boldsymbol{z})}{\mathcal{N}^v_{\boldsymbol{u},\sigma}(\boldsymbol{z})}, 1\right)$

$\mathcal{S}$**:**

1. $\boldsymbol{u} \leftarrow h$
2. $\boldsymbol{z} \leftarrow \mathcal{N}^v_\sigma$
3. *output* $(\boldsymbol{u}, \boldsymbol{z})$ *with probability* $1/M$

Moreover, the probability that $\mathcal{A}$ outputs a value is at least $\frac{1-2^{-\omega(\log(v\nu))}}{M}$.

In [29], the author remarks that if $\sigma = \alpha T, \alpha > 0$ and $M = \exp\left(12/\alpha + 1/(2\alpha^2)\right)$ then the output of both algorithms will be within statistical distance $2^{-100}/M$ and $\mathcal{A}$ will output a value with probability at least $\frac{1-2^{-100}}{M}$. As an example, assume that we want the signing algorithm to succeed in each iteration with probability 1/3, i.e. we want to set $M = 3$. Then following the reasoning in [29], we can set $\sigma = 11 \cdot T$. This means that the output of the signing algorithm is indistinguishable from the simulator except with probability $\approx 2^{-98}$, which we deem sufficient for our application.

2.2 Module-SIS and Module-LWE

The security of our linkable ring signature scheme will be based on the hardness of two problems, Module-SIS and Module-LWE [24]. These problems are variants of the well-known SIS [1] and LWE [39] problems, but over modules that are defined over polynomial rings. This is a generalized version of the Ring-SIS and Ring-LWE problems [30,31,38]. Using Module-lattice assumptions comes with two advantages: (i) while they are a generalization of ideal-lattice assumptions, they still retain some structure which is necessary to construct a large space of short, invertible elements which is necessary for our construction; and (ii) there is evidence that module lattices of larger rank are less prone to certain attacks than ideal-lattices [3,8].

The homogeneous Module-SIS problem consists of finding a vector $\boldsymbol{r}$ of small norm such that $\boldsymbol{Ar} = 0$ for a given, structured matrix $\boldsymbol{A}$.

Definition 1 ($\text{MSIS}_{h,v,t}$). *Given* $\boldsymbol{A} \leftarrow R_q^{h \times v}$, *find* $\boldsymbol{r} \in R^v$ *such that* $\boldsymbol{Ar} = 0$ *and* $0 < \|\boldsymbol{r}\|_2 \leq t$.

Our scheme also uses the Decisional Module-LWE problem. In D-MLWE, the problem consists of distinguishing noisy linear equations from random.

Definition 2 ($\text{D-MLWE}_{h,v,\beta}$). *Let* $\boldsymbol{A} \leftarrow R_q^{h \times v}$. *Then distinguish the distributions*

$$(\boldsymbol{A}, \boldsymbol{Ar}) \quad \textit{and} \quad (\boldsymbol{A}, \boldsymbol{u})$$

where $\boldsymbol{r} \leftarrow S_\beta^v$ *and* $\boldsymbol{u} \leftarrow R_q^h$.

Here, we use a special instance of the Module-LWE problem where the secret has the same distribution as the noise[2].

If two samples (with different matrices, but same secret vector $\boldsymbol{r}$) are issued by the challenger, then this can still be related to a D-MLWE instance but with different parameters, as the following proposition shows.

Proposition 1. *Let* $\boldsymbol{A}, \boldsymbol{B} \leftarrow R_q^{h \times v}$, $\boldsymbol{r} \leftarrow S_\beta^v$ *and* $\boldsymbol{c}, \boldsymbol{d} \leftarrow R_q^h$. *Then*

$$(\boldsymbol{A}, \boldsymbol{Ar}, \boldsymbol{B}, \boldsymbol{Br}) \approx_c (\boldsymbol{A}, \boldsymbol{c}, \boldsymbol{B}, \boldsymbol{d})$$

given the $\text{D-MLWE}_{2h,v,\beta}$*-problem is hard.*

Proof. Consider the matrices $\boldsymbol{E} = \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{B} \end{bmatrix}$, and $\boldsymbol{Er} = \begin{bmatrix} \boldsymbol{Ar} \\ \boldsymbol{Br} \end{bmatrix}$. Then distinguishing the above distributions is equivalent to distinguishing

$$(\boldsymbol{E}, \boldsymbol{Er}) \approx_c \left(\boldsymbol{E}, \begin{bmatrix} \boldsymbol{c} \\ \boldsymbol{d} \end{bmatrix} \right)$$

This is the definition of the $\text{D-MLWE}_{2h,v,\beta}$ problem. □

[2] This equivalent formulation is possible in our setting, as only one LWE sample will be issued per secret. The definition might seem unusual at first, as one regularly defines the LWE distribution as $\boldsymbol{As}_1 + \boldsymbol{s}_2$. We can use the following transformation, which is well-known: note that the given equation is equivalent to writing $\boldsymbol{As}_1 + \boldsymbol{I}_h \boldsymbol{s}_2$ instead. By aligning this into a single matrix product of $\boldsymbol{A}'$ with $(\boldsymbol{s}_1 | \boldsymbol{s}_2)$ and multiplying the resulting challenge with a uniformly random $r \in R_q$, we obtain Definition 2.

Our construction will moreover rely on a third problem, namely the Search Module-LWE problem. It can be seen as an inhomogeneous MSIS instance where the target is known to have a short preimage under $\boldsymbol{A}$.

Definition 3 (S-MLWE$_{h,v,\beta}$). *Sample a uniformly random* $\boldsymbol{r} \leftarrow S_\beta^v$. *Given* $\left(\boldsymbol{A} \leftarrow R_q^{h\times v};\ \boldsymbol{s} = \boldsymbol{A}\boldsymbol{r}\right)$ *find* $\boldsymbol{r}' \in R^v$ *such that* $\boldsymbol{A}\boldsymbol{r}' = \boldsymbol{s}$ *and* $0 < \|\boldsymbol{r}'\|_\infty \leq \beta$.

Fixing h, v, β of an S-MLWE-instance, it is easy to see that any algorithm $\mathcal{A}$ that solves S-MLWE-instances can also solve D-MLWE-instances with the same parameters in comparable time and with similar probability. For the converse direction, Langlois and Stehlé [24] showed that, for certain parameter sets, S-MLWE can be reduced to D-MLWE.

2.3 Linkable Ring Signatures

The formal syntax and security model of linkable ring signatures, sometimes also called linkable spontaneous anonymous group signatures, can be found in [17,27]. Definitions of linkable ring signatures with adaptation to the cryptocurrency scenario can be found in [37]. Our definitions are in the spirit of [17,20,27].

Definition 4 (Linkable Ring Signature). *A linkable ring signature scheme consists of five algorithms:*

Setup(1^λ)**:** *Generates and outputs public parameters PP available to all users.*
KGen(PP)**:** *Generates a public key PK and a private signing key SK.*
Sign$_{PP,SK_\ell}(m, L)$**:** *Outputs a signature* Ω *on the message* $m \in \{0,1\}^\star$ *with respect to the ring* $L = (PK_1, \ldots, PK_N)$. *Here,* (PK_ℓ, SK_ℓ) *is a valid key pair output by* **KGen**(PP), *and* $PK_\ell \in L$.
Vfy(m, L, Ω)**:** *Verifies a purported ring signature* Ω *on a message m with respect to the ring of public keys L. It outputs a bit* $b \in \{0,1\}$.
Link$(m_1, m_2, \Omega_1, \Omega_2)$[3]**:** *Takes as inputs two messages* m_1, m_2 *as well as two signatures* Ω_1 *and* Ω_2 *and outputs* $b \in \{0,1\}$.

The above algorithms form a linkable ring signature scheme if the following three definitions of correctness, signer anonymity, linkability and exculpability are fulfilled.

Definition 5 (Correctness). *Let* $N \geq 1$. *Then* $\forall t \in [N]$, $\forall\{i_1, \ldots, i_t\} \subset [N], k \in \{i_1, \ldots, i_t\}$ *and* $\forall m \in \{0,1\}^*$ *it holds that*

$$\Pr\left[\mathbf{Vfy}(m, L, \Omega) = 0 \;\middle|\; \begin{array}{l} PP \leftarrow \mathbf{Setup}(), \\ \{PK_i \leftarrow \mathbf{KGen}(PP)\}_{i\in[N]}, \\ L = (PK_{i_1}, \ldots, PK_{i_t}), \\ \Omega = \mathbf{Sign}_{PP,SK_k}(m, L) \end{array}\right] \leq \mathrm{negl}(\lambda)$$

[3] Different from the definition of **Link** algorithm in the existing linkable ring signature schemes [17,27], our definition does not take L as inputs since we are talking about one-time linkable ring signature.

Signer anonymity captures the intuition that if the targeted signer is not corrupted, then the probability that the adversary can identify him as the true signer among all uncorrupted parties is negligible.

Definition 6 (Signer Anonymity). *Let $L = (PK_1, \ldots, PK_N)$ be a list of public keys and D_t be any set of $0 \leq t < N$ signing keys such that $\forall SK_i \in D_t \; \exists PK_i \in L : \; (PK_i, SK_i)$ is generated by* **KGen**. *A ring signature scheme is signer anonymous if for any PPT algorithm $\mathcal{E}$, on inputs of any message m, sets L, D_t as defined above and any valid signature Ω on L and m generated using $SK_\ell \notin D_t$, then*

$$\left| \Pr\left[\mathcal{E}\left(m, L, D_t, \Omega\right) = \ell\right] - \frac{1}{N-t} \right| \leq \mathrm{negl}(\lambda).$$

Let $PP \leftarrow \mathbf{Setup}(1^\lambda)$. For the following two definitions we assume the existence of two oracles $\mathcal{O}_K, \mathcal{O}_S$:

Key generation oracle $\mathcal{O}_K$: On input of a bit b generate a random keypair $(PK, SK) \leftarrow \mathbf{KGen}(PP)$. If $b = 0$ then output PK, otherwise (PK, SK).

Signing oracle $\mathcal{O}_S$: On input (L, m, i) where $L = (PK_1, \ldots, PK_N)$ are public keys generated by $\mathcal{O}_K$, $i \in [N]$ and $\mathcal{O}_K$ did not output SK_i and $m \in \{0,1\}^*$, return $\Omega \leftarrow \mathbf{Sign}_{PP, SK_i}(m, L)$. If a key in L was not queried before, then output $\perp$.

The idea behind the Linkability definition is as follows: if the same signer generates two signatures, then the algorithm **Link** will identify this with overwhelming probability. It is important that this not only holds against honest use of the algorithm **Sign**, but arbitrary adversaries.

Definition 7 (Linkability). *Let $\mathcal{A}$ be a PPT algorithm with oracle access to $\mathcal{O}_K, \mathcal{O}_S$. $\mathcal{A}$ is given 1^λ and PP as input and outputs a list $L \subseteq \overline{L}$ (where $\overline{L}$ is the set of all keys queried from $\mathcal{O}_K$) of length N together with $N+1$ values $\{(m_i, \Omega_i)\}_{i \in [N+1]}$. Then the scheme is linkable if, for every such $\mathcal{A}$,*

$$\Pr\begin{bmatrix} \forall i \in [N+1] : \mathbf{Vfy}(m_i, L, \Omega_i) = 1, \\ \forall i, j \in [N+1],\, i \neq j : \mathbf{Link}(m_i, m_j, \Omega_i, \Omega_j) = 0 \end{bmatrix} \leq \mathrm{negl}(\lambda).$$

The above only talks about the setting of generating signatures without being traceable. Equally important is the setting where signatures are signed by two different parties, where we require that their tags must be distinct. This then, of course, in particular includes the case of the **Sign** algorithm. This property is important in the setting of cryptocurrencies where one might otherwise be able to issue fake transactions on behalf of another party.

Definition 8 (Exculpability). *Let $\mathcal{A}$ be a PPT algorithm with oracle access to $\mathcal{O}_K, \mathcal{O}_S$. $\mathcal{A}$ is given 1^λ and PP as input and outputs a list $L \subseteq \overline{L}$ (where $\overline{L}$ is the set of all keys queried from $\mathcal{O}_K$) of length N together with two pairs $(m_1, \Omega_1), (m_2, \Omega_2)$ with $\mathbf{Vfy}(m_1, L, \Omega_1) = \mathbf{Vfy}(m_2, L, \Omega_2) = 1$, not both queried to $\mathcal{O}_S$. Let $M \subset L$ be set of PK_i for which $\mathcal{A}$ did not obtain SK_i from $\mathcal{O}_K$. Then*

$$\Pr\left[\mathbf{Link}(L, m_1, m_2, \Omega_1, \Omega_2) = 1 \;\middle|\; \begin{array}{l} \exists PK_i \in M, \exists m \in \{0,1\}^*, \\ \exists j \in \{1,2\} : \\ \left[\Omega \leftarrow \mathbf{Sign}_{PP,SK_i}(m, L),\right. \\ \left.\mathbf{Link}(m, m_j, \Omega, \Omega_j) = 1\right] \end{array}\right] \leq \mathrm{negl}(\lambda).$$

Remark 2. In our scheme, we do not give a definition and proof for existential unforgeability. As was observed in [17] the above definitions imply this property, as any algorithm breaking existential unforgeability can be used in a black-box setting to break exculpability (see [17, Theorem 2.6]).

3 Constructing Linkable Ring Signatures

In this section, we will describe our linkable ring signature scheme and prove its security. Our proposed scheme can be considered as an adaption of the linkable ring signature scheme proposed in [27] to the lattice setting. However, while most linkable signature schemes such as the one proposed in [16] require the use of a pseudorandom function to achieve linkability, our scheme demonstrates that the linkability for one-time ring signature schemes can be obtained without using a pseudorandom function to generate the tag.

If a scheme is not one-time, then this PRF is evaluated on the secret (or public) key of the signing party and a description of the actual ring L. In our case, it is not necessary to include the ring L into the tag computation (as the scheme is one-time) and we attach a tag derived from the secret key only. Concretely, each party will have a private key $\boldsymbol{r}_i$ together with a public key $PK_i = \boldsymbol{A}\boldsymbol{r}_i$, where $\boldsymbol{A}$ is a random length-compressing matrix and $\boldsymbol{r}_i$ is a vector of small norm. Thus, PK_i is an evaluation of the public collision-resistant hash function $f_{\boldsymbol{A}}(\cdot) : \boldsymbol{x} \mapsto \boldsymbol{A}\boldsymbol{x}$ on the private input $\boldsymbol{r}_i$.

During the signing process, the signer will generate two rings of signatures (similar to [27,40] but twice): the first is a ring consisting of signatures for all the N public keys and generated using $f_{\boldsymbol{A}}$ whereas the second ring uses a different CRHF $f_{\boldsymbol{B}}$. This function $f_{\boldsymbol{B}}(\cdot) : \boldsymbol{x} \mapsto \boldsymbol{B}\boldsymbol{x}$ uses a different public matrix $\boldsymbol{B}$ having the same dimensions as $\boldsymbol{A}$. The crucial point to interleave these rings is that they are built simultaneously, using the same challenges and blinding value in each step. For this to be verifiable, the signer must now include his I_i in the signature, which serves the same purpose as the public key PK_i in the first ring. We will show that the signer is bound to use his own value I_i if he wants to generate a valid signature and will therefore produce a collision if a second signature is revealed.

Let $H : \{0,1\}^* \to D$ be a cryptographic hash function where D is the challenge space defined in Sect. 2. The algorithms of our scheme are defined as follows:

Setup(1^λ)**:** Sample two random matrices $\boldsymbol{A}, \boldsymbol{B} \leftarrow R_q^{h \times v}$ and set $PP = (\boldsymbol{A}, \boldsymbol{B})$.
KGen(PP)**:** Sample $\boldsymbol{r} \leftarrow S_\beta^v$ and then generate the public key $PK = \boldsymbol{A}\boldsymbol{r}$ as well as the signing key $SK = \boldsymbol{r}$.
Sign$_{PP,SK_\ell}(m, L)$**:**

1. Compute the tag $I_\ell = \boldsymbol{B}\boldsymbol{r}_\ell$.
2. Sample $\boldsymbol{u} \leftarrow \mathcal{N}_\sigma^v$ and set $d_{\ell+1} \leftarrow H(L, I_\ell, m, \boldsymbol{A}\boldsymbol{u}, \boldsymbol{B}\boldsymbol{u})$.
3. For each $i = \ell + 1, \ldots, N, 1, \ldots, \ell - 1$:
   (a) Sample $\boldsymbol{r}_{z,i} \leftarrow \mathcal{N}_\sigma^v$.
   (b) Set $t_{i,1} = \boldsymbol{A}\boldsymbol{r}_{z,i} - d_i PK_i$ and $t_{i,2} = \boldsymbol{B}\boldsymbol{r}_{z,i} - d_i I_\ell$ as well as $d_{(i \mod N)+1} \leftarrow H(L, I_\ell, m, t_{i,1}, t_{i,2})$.
4. Compute $\boldsymbol{r}_{z,\ell} = \boldsymbol{u} + d_\ell \boldsymbol{r}_\ell$.
5. Abort with probability $1 - \min\left(1, \frac{\mathcal{N}_\sigma^v(\boldsymbol{r}_{z,\ell})}{M \cdot \mathcal{N}_{d_\ell \boldsymbol{r}_\ell, \sigma}^v(\boldsymbol{r}_{z,\ell})}\right)$, otherwise output the signature $\Omega = \left(d_1, (\boldsymbol{r}_{z,i})_{i \in [N]}, I_\ell\right)$.

Vfy(m, L, Ω)**:**

1. For $i \in [N]$, check whether $\|\boldsymbol{r}_{z,i}\|_2 \leq 2\sigma\sqrt{\nu v}$, else output 0.
2. For $i \in [N]$, compute $t'_{i,1} = \boldsymbol{A}\boldsymbol{r}_{z,i} - d_i PK_i$, $t'_{i,2} = \boldsymbol{B}\boldsymbol{r}_{z,i} - d_i I_\ell$ as well as $d_{i+1} = H\left(L, I_\ell, m, t'_{i,1}, t'_{i,2}\right)$.
3. If $d_1 = H\left(L, I_\ell, m, t'_{N,1}, t'_{N,2}\right) = d_{N+1}$ then output 1, else output 0.

Link(Ω_1, Ω_2)**:** Given

$$\Omega_1 = \left(d_1^{(1)}, \left(\boldsymbol{r}_{z,i}^{(1)}\right)_{i \in [N]}, I_\ell^{(1)}\right) \text{ and } \Omega_2 = \left(d_1^{(2)}, \left(\boldsymbol{r}_{z,i}^{(2)}\right)_{i \in [N]}, I_\ell^{(2)}\right),$$

return 1 if $I_\ell^{(1)} = I_\ell^{(2)}$ and 0 otherwise.

Correctness can easily be verified using Lemmas 1 and 2.

3.1 Security

We now give the security statements of our construction. Due to length constraints, the proofs for these can be found in Appendix A.

Theorem 1 (Signer Anonymity). *The proposed ring signature scheme provides signer anonymity in the (programmable) random oracle model assuming hardness of the* D-MLWE$_{2h,v,\beta}$*-problem.*

Theorem 2 (Linkability). *Assume that there exists an algorithm $\mathcal{A}$ that breaks linkability with probability ϵ, in time at most s, with at most q_H queries to $\mathcal{O}_K$ and q_S queries to $\mathcal{O}_S$. Then there exists an algorithm $\mathcal{M}$ that breaks a* MSIS$_{h,v,t}$*-instance with probability* $\left(\epsilon - \frac{1}{|\overline{D}|^{-q_H - Nq_S}}\right)^2 / \left((N^2+N)q_H\right)^2$ *in time* $O(N^2 \cdot q_H \cdot s)$ *where* $t = 4\sigma\sqrt{v \cdot \nu} + 2 \cdot \kappa \cdot v \cdot \nu^{1.5} \cdot \beta$.

Theorem 3 (Exculpability). *Assume that there exists an algorithm $\mathcal{A}$ that breaks exculpability with probability ϵ, in time at most s, with at most q_H queries to $\mathcal{O}_K$ and q_S queries to $\mathcal{O}_S$. Then there exists an algorithm $\mathcal{M}$ that either breaks an* S-MLWE$_{2h,v,\beta}$ *instance or an* MSIS$_{h,v,t}$*-instance with probability*

$$\left(\frac{(N-1)\epsilon}{N} - \frac{1}{|\overline{D}| - q_H - Nq_S}\right)^2 / \left((N^2+N)(q_H + N \cdot q_S)\right)^2$$

in time $O(N \cdot q_H \cdot s)$ where $t = 4\sigma\sqrt{v \cdot \nu} + 2 \cdot \kappa \cdot v \cdot \nu^{1.5} \cdot \beta$.

4 Discussion

We now discuss questions surrounding the practicality of our scheme and hint at future research directions.

Practical Considerations. The runtime of **Vfy** is essentially the N-fold runtime of the verification of a regular lattice-based signature scheme. For signing, the computation and sampling of $I_\ell, \boldsymbol{u}$ as well as $\boldsymbol{r}_{r,j}, \boldsymbol{Ar}_{z,j}, \boldsymbol{Br}_{z,j}$ for $j \neq \ell$ can be done offline. The size of the total signature is approximately the size of N individual lattice-based signatures, as can be seen in Table 2.

As the basis of our construction, we chose a simple signature scheme without optimizations. Following the outline of our algorithms, one can instantiate it with e.g. [14] and then use their key-compression technique: this optimization is important when it comes to signature size.

Parameter Selection. In our construction, the D-MLWE-instance from Theorem 1 and the S-MLWE-instance in Theorem 3 have the same dimensions and bounds. Moreover, it was already mentioned in Sect. 2.2 that any algorithm which solves the S-MLWE problem in time h with success probability ϵ can be turned into a distinguisher for D-MLWE for the same dimension with essentially the same runtime and success probability. It thus suffices in the parameter selection to look at the D-MLWE-instance only.

Unfortunately, it seems like the security reduction cannot be used for the choice of parameters, as it is inherently non-tight: from the proofs in Sect. 3, we see that the reductions have a huge loss in terms of success probability (both due to the use of the Forking Lemma and because the runtime is proportional to the number of queries of $\mathcal{A}$ to H). If one attempts to obtain a good success probability of the reduction, the estimated runtime gets rather large. We leave a proof with a tighter reduction that can be used to instantiate our construction as an open problem.

Instead, we chose the parameters of our scheme such that the MSIS, D-MLWE-problems are hard given that the reduction succeeds (see Table 2). As baseline, we assume hardness of at least 128 bits using all currently known lattice reduction attacks. This is reflected by requiring that lattice reduction will have to achieve a Root Hermite factor of less than 1.003 to break our

Table 2. Parameter settings for our scheme

Parameter	Recommended choice
q	$\approx 2^{32}$
ν	1024
h	1
v	4
κ	45/90
β (in S_β)	1
σ	31680/63360
t (ℓ_2 MSIS-bound)	$\approx 2^{24}/2^{25}$
Root Hermite factor	$<$1.0030
Public key size (per party)	$\approx$8 KB/8 KB
Signing key size (per party)	$\approx$8.8 KB/8.8 KB
Signature ($N = 1$)	$\approx$17.4 KB/17.9 KB
Signature ($N = 8$)	$\approx$82.5 KB/86.5 KB
Signature ($N = 32$)	$\approx$305.7 KB/321.7 KB
Signature ($N = 128$)	$\approx$1.17 MB/1.23 MB

scheme. For the given parameters, the security relies only on Module-SIS/LWE with $h = 1$ i.e. Ring-SIS/LWE, but increasing h, v, κ and thus decreasing ν would allow to base the hardness on Module-SIS/LWE with a larger rank with only a minor increase in the size of the signature.

To choose actual parameters, we use the LWE simulator with sparse secrets from [2,4] for D-MLWE. Moreover, we use [34] to assess the hardness of our obtained SIS instance[4]. The size estimates in Table 2 are in Kilobytes/Megabytes (as in related work), we bound the size of each coefficient of $\boldsymbol{r}_{z,i}$ assuming it is within a 6σ-interval.

Post-Quantum Security. It is widely believed that hardness assumptions used in our scheme may offer security in a post-quantum era. On the other hand, it is unlikely that our security proofs carry over to the Quantum Random Oracle Model (QROM, see e.g. [7]): we use adaptive programming of the RO H in Theorem 1, and adaptive rewinding in Theorems 2 and 3. Both of these proof techniques are somewhat inherent to the construction.

[4] While there might be newer methods to assess the hardness of SIS more precisely, [34] suffices for an estimation of parameters. Moreover, it turned out that using different methods yields hardness estimates (in terms of the Root Hermite factor) that are very close to [34]. Our parameter choices were considered secure at the time of writing, but the reader should refer to the full version of this work for updated parameters.

We note that other candidate constructions in the QROM such as [11,14] also use a form of RO programming (even though not adaptively). Moreover, though it seems unlikely that the Forking Lemma can be proven in the QROM, there exist no attacks on protocols using these proof techniques which stem from this use of the RO, to the best of our knowledge.

A Proof of Security

A.1 Simulation

The simulation strategy follows a similar pattern as in [27,40]. In an honestly generated ring signature (where the secret key SK_ℓ is known) the **Sign** algorithm simulates $N-1$ individual signatures consecutively for all public keys but the one to which its secret key SK_ℓ belongs. For this last public key, it uses the challenge d_ℓ that is obtained for the last signature to *close the ring* using the secret key SK_ℓ. A simulator has no secret key and will instead generate all N individual signatures consecutively this way. To close the ring, it needs to reprogram the random oracle H on the last query to exactly yield the challenge d_1 that is necessary to make all tests in **Vfy** go through. Even though this reprogramming takes place, the challenge d_1 that the RO returns will be fixed in the simulation ahead of time but be chosen uniformly at random. This means that the reprogramming is not detectable. Furthermore, Lemma 2 ensures that the simulation of the ring is indistinguishable.

Concerning the simulation and consistency of the second ring which involves I we note that here I is not obtained from the same secret input $\boldsymbol{r}$ that is used to derive PK from $\boldsymbol{A}$ since the simulator does not know SK. Instead, it will choose this value I uniformly at random from the appropriate set. An adversary cannot distinguish between I and the correctly generated counterpart due to Proposition 1.

In fact, the D-MLWE$_{2h,v,\beta}$ assumption of Proposition 1 attests to the indistinguishability of a pair of quadruples: $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\cdot\boldsymbol{r}, \boldsymbol{B}\cdot\boldsymbol{r}) \sim (\boldsymbol{A}, \boldsymbol{B}, u, v)$, where u, v are random. One can further reduce the indistinguishability of another pair of quadruples: $(\boldsymbol{A}, \boldsymbol{B}, u, v) \sim (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\cdot\boldsymbol{r}, v)$ to D-MLWE$_{h,v,\beta}$ problem, the hardness of which can be deduced from that of D-MLWE$_{2h,v,\beta}$. Based on hybrid argument, the indistinguishability of the following two quadruples $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\cdot\boldsymbol{r}, v) \sim (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{A}\cdot\boldsymbol{r}, \boldsymbol{B}\cdot\boldsymbol{r})$ is reduced to the D-MLWE$_{2h,v,\beta}$ assumption.

A.2 Linkability

Assume that a PPT algorithm $\mathcal{A}$ is run with some certain input and that it generates an output as in the linkability definition. $\mathcal{A}$ makes queries to both the random oracle H and to the two oracles $\mathcal{O}_K, \mathcal{O}_S$ in order to generate these signatures. We construct an algorithm $\mathcal{R}$ which will run $\mathcal{A}$ with multiple inputs and

will attempt to rewind it on one of these inputs with different outputs from the random oracle. During a run, $\mathcal{A}$ will be allowed to make q_H queries to the random oracle directly, but also $\mathcal{O}_S$ indirectly[5] makes $N \cdot q_S$ queries to H to generate all the queried signatures. $\mathcal{R}$ will simulate $H, \mathcal{O}_S, \mathcal{O}_K$ honestly and will rewind $\mathcal{A}$ with the goal of finding two signatures $\Omega, \hat{\Omega}$ that for some index $\pi \in [N]$ used in signature verification have the same RO query (L, I, m, t_π, t'_π), but differing $d, \hat{d}, \boldsymbol{r}, \hat{\boldsymbol{r}}$ which go into generating this query for each individual signature. Furthermore, we require that the used I has a public key PK_π that was not generated by the simulated oracle[6]. In the full version, we show how to construct such $\mathcal{R}$ that succeeds with probability $\left(\epsilon - \frac{1}{|\overline{D}|-q_H-Nq_S}\right)^2 / \left((N^2+N)q_H\right)^2$ in time $O(N^2 \cdot q_H \cdot s)$.

Using this algorithm $\mathcal{R}$, we construct another PPT TM $\mathcal{M}$. This algorithm will obtain a MSIS-challenge $\boldsymbol{A}$, use it as the matrix that generates public keys and uses $\mathcal{R}$ to compute the aforementioned signatures. We obtain $d, \hat{d}, \boldsymbol{r}, \hat{\boldsymbol{r}}, \pi$ such that $(d-\hat{d})PK_\pi = \boldsymbol{A}(\boldsymbol{r}-\hat{\boldsymbol{r}})$ and $(d-\hat{d})I = \boldsymbol{B}(\boldsymbol{r}-\hat{\boldsymbol{r}})$.

PK_π was generated honestly by $\mathcal{O}_K$ and we have $\boldsymbol{r}_\pi$ such that $PK_\pi = A\boldsymbol{r}_\pi$. Rewrite the above as $\boldsymbol{A}(d-\hat{d})\boldsymbol{r}_\pi = \boldsymbol{A}(\boldsymbol{r}-\hat{\boldsymbol{r}})$. Assume that $(d-\hat{d})\boldsymbol{r}_\pi = (\boldsymbol{r}-\hat{\boldsymbol{r}})$ then by the invertibility of $(d-\hat{d})$ it holds that $I_\pi = \boldsymbol{B}\boldsymbol{r}_\pi = \boldsymbol{B}\left((\boldsymbol{r}-\hat{\boldsymbol{r}}) \cdot (d-\hat{d})^{-1}\right) = I$ which contradicts the assumption that I is different from all honestly generated tags. Hence $(d-\hat{d})\boldsymbol{r}_\pi \neq (\hat{\boldsymbol{r}}-\boldsymbol{r})$ and thus $\boldsymbol{s} = (d-\hat{d})\boldsymbol{r}_\pi - (\hat{\boldsymbol{r}}-\boldsymbol{r}) \neq 0$, while $0 = \boldsymbol{A}\boldsymbol{s}$ which yields a solution $\boldsymbol{s}$ to the MSIS-instance as in Definition 1.

A.3 Exculpability

The algorithm $\mathcal{M}$ which we will construct in the course of this proof will either use the matrix $\boldsymbol{A}$ in **Setup** to implant an MSIS-challenge or alternatively choose $\boldsymbol{A}, \boldsymbol{B}$ from an S-MLWE instance. Whereas in the former case the proof works as above, in the latter one we use a randomly chosen public key and its corresponding tag to embed an S-MLWE challenge. This then means that we cannot correctly simulate the $\mathcal{O}_S$-oracle as we would need the secret key for it - which is the secret we want to extract! Instead, the proof uses a version of the simulator from signer anonymity.

With respect to the **Link** algorithm from our construction, the definition translates into the requirement that the tags $I^{(1)}, I^{(2)}$ from Ω_1, Ω_2 are equal. Moreover, each $I^{(i)}$ must be identical to an honestly generated identification tag for one of the public keys in L, and $\mathcal{A}$ did not obtain both signatures from $\mathcal{O}_S$ and does not possess the secret key for this public key. Let $I = I^{(1)} = I^{(2)}$.

[5] These indirect queries are not important when we discuss a signature that does not correspond to any public key.

[6] We will describe the explicit construction of $\mathcal{R}$ in the full version of this work, but it follows a standard approach using a version of the Forking Lemma.

The algorithm $\mathcal{M}$ will first fairly flip a bit $b \leftarrow \mathcal{B}_{1/2}$. Then it does the following, based on the value of b:

$b = 0$**:** $\mathcal{M}$ will take a S-MLWE instance $(\boldsymbol{D}, \boldsymbol{t})$ where $\boldsymbol{D} = \begin{pmatrix} \boldsymbol{A} \\ \boldsymbol{B} \end{pmatrix} \in R_q^{2h \times v}$ and $\boldsymbol{t} = \begin{pmatrix} \boldsymbol{t}_0 \\ \boldsymbol{t}_1 \end{pmatrix} \in R_q^{2h}$ such that $\boldsymbol{A}, \boldsymbol{B} \in R_q^{h \times v}$ and $\boldsymbol{t}_0, \boldsymbol{t}_1 \in R_q^h$. Assign $PP = (\boldsymbol{A}, \boldsymbol{B})$ and choose an index $k \in [N]$. For $j \in [N]$ set

$$(PK_j, SK_j) = \begin{cases} (\boldsymbol{A}\boldsymbol{r}_j, (\boldsymbol{r}_j, \boldsymbol{B}\boldsymbol{r}_j)) & \text{if } k \neq j \text{ and for } \boldsymbol{r}_j \leftarrow S_\beta^v \\ (\boldsymbol{t}_0, (\perp, \boldsymbol{t}_1)) & \text{if } k = j \end{cases}$$

We then set the counter $j = 1$. Whenever $\mathcal{A}$ requests a public key from $\mathcal{O}_K$, then output PK_j and increase j by 1. If $j = k$ and $\mathcal{A}$ requests the secret key then abort. Whenever $\mathcal{O}_S$ is queried, then sign the signature for the queried key s correctly if $s \neq k$, otherwise use the back-patching simulator from the Signer Anonymity proof[7], but with $I_j = \boldsymbol{t}_1$.

$b = 1$**:** $\mathcal{M}$ will take a MSIS instance $\boldsymbol{A} \in R_q^{h \times v}$ as input, sample $\boldsymbol{B} \leftarrow R_q^{h \times v}$ uniformly at random and set $PP = (\boldsymbol{A}, \boldsymbol{B})$. It will additionally choose $k \in [N]$ uniformly at random. $\mathcal{O}_K$ will generate all keys honestly, but abort if $\mathcal{A}$ queries SK_k. $\mathcal{O}_S$ will run **Sign** honestly.

Assume that $\mathcal{A}$ does not query for SK_k, then the output of $\mathcal{A}$ will be independent of the choice of b due to Theorem 1. If $b = 0$ then $\mathcal{A}$ will be stopped if SK_k is queried, but observe that this abort probability is the same in case $b = 1$ as the key PK_k is perfectly indistinguishable from honestly generated public key PK_j. Moreover, the abort probability in the presence of $\mathcal{O}_S$ is identical due to the construction of the oracle, so the probability that $\mathcal{A}$ outputs something is independent of b. This output probability is $\epsilon' = \epsilon \cdot (N-1)/N$ by the random choice of k.

In the next step, $\mathcal{M}$ now runs $\mathcal{A}$ using the algorithm $\mathcal{R}'$ (similar to $\mathcal{R}$ from the previous proof it implements a Forking Lemma-type algorithm) which succeeds with probability $\left(\epsilon - \frac{1}{|\overline{D}| - q_H - Nq_S}\right)^2 / \left((N^2+N)(q_H + N \cdot q_S)\right)^2$ in time $O(N \cdot q_H \cdot s)$ to obtain signatures that have identical inputs to the random oracle. From $\mathcal{R}'$ obtain values $d, \hat{d}, \boldsymbol{r}, \hat{\boldsymbol{r}}, \pi$ such that $(d - \hat{d})\boldsymbol{A}\boldsymbol{r}_\pi = (d - \hat{d})PK_\pi = \boldsymbol{A}(\boldsymbol{r} - \hat{\boldsymbol{r}})$ and $(d - \hat{d})I = \boldsymbol{B}(\boldsymbol{r} - \hat{\boldsymbol{r}})$ where $\boldsymbol{r}_\pi$ is the secret key belonging to PK_π. We might either have that $(d - \hat{d})\boldsymbol{r}_\pi = \boldsymbol{r} - \hat{\boldsymbol{r}}$ or that inequality holds. Now if the values are not equal, then we can use the same argument as in linkability to extract a MSIS solution (this covers the case when $b = 1$). But in case of equality the approach does not work - unless we are in the setting where the algorithm $\mathcal{M}$ chose $b = 0$. Now we know that equality holds and $\boldsymbol{r}_\pi$ is known to exist as PK_π is a S-MLWE challenge, which we can therefore extract.

[7] The anonymity simulation does only provide computational indistinguishability as it uses Proposition 1. Here the correctly generated I_j is known and the simulation is statistically indistinguishable, not just computationally.

More formally, if $b = 0$ and $k = \pi$ then $\mathcal{M}$ will output $\boldsymbol{r}_\pi = (\boldsymbol{r} - \hat{\boldsymbol{r}}) \cdot (d - \hat{d})^{-1}$ as $d - \hat{d} \in D'$. If $b = 1$ then it will instead output $(d - \hat{d})\boldsymbol{r}_\pi + \hat{\boldsymbol{r}} - \boldsymbol{r}$. We now calculate the probability that the algorithm $\mathcal{M}$ will output a correct answer to either of the two challenges. Therefore, denote with $\mathsf{X}_=$ the event that $(d - \hat{d})\boldsymbol{r}_\pi = \boldsymbol{r} - \hat{\boldsymbol{r}}$, and with $\mathsf{X}_\neq$ the opposite event. Let M denote the event that $\mathcal{M}$ outputs something. As our goal is to lower-bound the probability that the output of $\mathcal{M}$ is correct, we need to determine

$$\Pr\left[\mathcal{M} \text{ gives correct output}\right] = \Pr\left[\mathsf{X}_=, b = 0 | \mathsf{M}\right] + \Pr\left[\mathsf{X}_\neq, b = 1 | \mathsf{M}\right]$$

If $b = 0$, then by the choice of k, the probability that $\pi = k$ is at least $1/|L|$ and therefore $\Pr\left[\mathsf{M} | \mathsf{X}_=, b = 0\right] \geq 1/N$. Using Bayes' Theorem, we obtain that

$$\begin{aligned}
\Pr\left[\mathsf{X}_=, b = 0 | \mathsf{M}\right] &= \frac{\Pr\left[\mathsf{M} | \mathsf{X}_=, b = 0\right] \cdot \Pr\left[\mathsf{X}_=, b = 0\right]}{\Pr\left[\mathsf{M}\right]} \\
&\geq \Pr\left[\mathsf{M} | \mathsf{X}_=, b = 0\right] \cdot \Pr\left[\mathsf{X}_=, b = 0\right] \\
&\geq 1/N \cdot \Pr\left[\mathsf{X}_=\right] \cdot \Pr\left[b = 0\right] = 1/2N \cdot \Pr\left[\mathsf{X}_=\right]
\end{aligned}$$

where we use in the last step that the occurrence of $\mathsf{X}_=$ is independent of b.

In case of $b = 1$ we always give output, so we have that $\Pr\left[\mathsf{M} | \mathsf{X}_\neq, b = 1\right] = 1$. Using the same reasoning as above, we obtain that $\Pr\left[\mathsf{X}_\neq, b = 1 | \mathsf{M}\right] \geq 1/2 \cdot \Pr\left[\mathsf{X}_\neq\right]$ which yields an overall bound of $\Pr\left[\mathcal{M} \text{ gives correct output}\right] \geq 1/2N$.

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: STOC, pp. 99–108 (1996)
2. Albrecht, M.R., et al.: Estimate all the LWE, NTRU schemes! (2018). https://eprint.iacr.org/2018/331
3. Albrecht, M.R., Deo, A.: Large modulus ring-LWE ≥ module-LWE. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 267–296. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_10
4. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. J. Math. Cryptol. **9**(3), 169–203 (2015)
5. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 194–211. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_19
6. Bender, A., Katz, J., Morselli, R.: Ring signatures: stronger definitions, and constructions without random oracles. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 60–79. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_4
7. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_3
8. Bos, J., et al.: CRYSTALS - kyber: a CCA-secure module-lattice-based KEM (2017). https://eprint.iacr.org/2017/634

9. Boyen, X.: Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 499–517. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_29
10. Brakerski, Z., Kalai, Y.T.: A framework for efficient signatures, ring signatures and identity based encryption in the standard model (2010). http://eprint.iacr.org/2010/086
11. del Pino, R., Lyubashevsky, V., Neven, G., Seiler, G.: Practical quantum-safe voting from lattices. In: CCS 2017 (2017)
12. Derler, D., Ramacher, S., Slamanig, D.: Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives. In: Lange, T., Steinwandt, R. (eds.) PQCrypto 2018. LNCS, vol. 10786, pp. 419–440. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-79063-3_20
13. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in *Ad Hoc* groups. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 609–626. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_36
14. Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehle, D.: Crystals - dilithium: Digital signatures from module lattices (2017). http://eprint.iacr.org/2017/633
15. Ducas, L., Micciancio, D.: Improved short lattice signatures in the standard model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 335–352. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_19
16. Franklin, M., Zhang, H.: A framework for unique ring signatures (2012). http://eprint.iacr.org/2012/577
17. Fujisaki, E., Suzuki, K.: Traceable ring signature. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 181–200. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_13
18. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC, pp. 197–206. ACM (2008)
19. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 112–131. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052231
20. Groth, J., Kohlweiss, M.: One-out-of-many proofs: or how to leak a secret and spend a coin. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 253–280. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_9
21. Güneysu, T., Lyubashevsky, V., Pöppelmann, T.: Practical lattice-based cryptography: a signature scheme for embedded systems. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 530–547. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33027-8_31
22. Hoffstein, J., Pipher, J., Silverman, J.H.: NSS: an NTRU lattice-based signature scheme. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 211–228. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_14
23. Katz, J., Kolesnikov, V., Wang, X.: Improved non-interactive zero knowledge with applications to post-quantum signatures (2018). https://eprint.iacr.org/2018/475
24. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. **75**(3), 565–599 (2015)

25. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 1–31. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_1
26. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based PRFs and applications to e-cash. ASIACRYPT 2017 (2017). http://eprint.iacr.org/2017/856
27. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable and anonymous signature for ad hoc groups. In: ACISP 2004. LNCS, vol. 3108, pp. 325–335. Citeseer (2004)
28. Lyubashevsky, V.: Fiat-Shamir with aborts: applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_35
29. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_43
30. Lyubashevsky, V., Micciancio, D.: Generalized compact Knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_13
31. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1
32. Lyubashevsky, V., Seiler, G.: Partially splitting rings for faster lattice-based zero-knowledge proofs. In: EUROCRYPT 2018 (2018). https://eprint.iacr.org/2017/523
33. Aguilar Melchor, C., Bettaieb, S., Boyen, X., Fousse, L., Gaborit, P.: Adapting Lyubashevsky's signature schemes to the ring signature setting. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 1–25. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38553-7_1
34. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography, pp. 147–191. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-540-88702-7_5
35. Mohamed, M.S.E., Petzoldt, A.: RingRainbow – an efficient multivariate ring signature scheme. In: Joye, M., Nitaj, A. (eds.) AFRICACRYPT 2017. LNCS, vol. 10239, pp. 3–20. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-57339-7_1
36. Nguyen, L.: Accumulators from bilinear pairings and applications. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 275–292. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_19
37. Noether, S., Mackenzie, A.: Ring confidential transactions. Ledger **1**, 1–18 (2016)
38. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_8
39. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84–93 (2005)
40. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_32

41. Torres, W.A., et al.: Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1.0) (2018). https://eprint.iacr.org/2018/379
42. Tsang, P.P., Wei, V.K.: Short linkable ring signatures for e-voting, e-cash and attestation. In: Deng, R.H., Bao, F., Pang, H.H., Zhou, J. (eds.) ISPEC 2005. LNCS, vol. 3439, pp. 48–60. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-31979-5_5
43. Wang, J., Sun, B.: Ring signature schemes from lattice basis delegation. In: Qing, S., Susilo, W., Wang, G., Liu, D. (eds.) ICICS 2011. LNCS, vol. 7043, pp. 15–28. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25243-3_2
44. Yang, R., Au, M.H., Lai, J., Xu, Q., Yu, Z.: Lattice-based techniques for accountable anonymity: composition of abstract Stern's protocols and weak PRF with efficient protocols from LWR. Cryptology ePrint Archive, Report 2017/781 (2017)