entropy

MDPI

Article

Lattice-Based Logarithmic-Size Non-Interactive Deniable Ring Signatures

Huiwen Jia [1], Chunming Tang [1,*] and Yanhua Zhang [2,*]

[1] School of Mathematics and Information Science, Guangzhou University, No. 230 Wai Huan Xi Road, Guangzhou 510006, China; hwjia@gzhu.edu.cn
[2] College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
* Correspondence: ctang@gzhu.edu.cn (C.T.); yhzhang@zzuli.edu.cn (Y.Z.)

Abstract: Deniable ring signature can be regarded as group signature without group manager, in which a singer is capable of singing a message anonymously, but, if necessary, each ring member is allowed to confirm or disavowal its involvement in the signature via an interactive mechanism between the ring member and the verifier. This attractive feature makes the deniable ring signature find many applications in the real world. In this work, we propose an efficient scheme with signature size logarithmic to the cardinality of the ring. From a high level, we adapt Libert et al.'s zero-knowledge argument system (Eurocrypt 2016) to allow the prover to convince the verifier that its witness satisfies an additional condition. Then, using the Fait-Shamir transformation, we get a non-interactive deniable ring signature scheme that satisfies the anonymity, traceability, and non-frameability under the small integer solution assumption in the random oracle model.

Keywords: deniable ring signature; zero-knowledge protocols; accumulators

Citation: Jia, H.; Tang, C.; Zhang, Y. Lattice-Based Logarithmic-Size Non-Interactive Deniable Ring Signatures. *Entropy* **2021**, *23*, 980. https://doi.org/10.3390/e23080980

Academic Editors: Amin Sakzad and Khoa Nguyen

Received: 10 June 2021
Accepted: 28 July 2021
Published: 29 July 2021

1. Introduction

Ring signature was first formalized by Rivest et al. [1] to deal with situations, such as leaking secrets anonymously. Specifically, a signer first picks up several public keys to form a ring; then, it generates a signature anonymously on behalf of the ring using its secret key. Any verifier is unable to get any information about the real signer, except that the message is signed by one of the ring member. This appealing feature has made the ring signature find various applications in cryptography [1–3]. In some situations, however, the anonymity feature is not always desirable, as it allows a user who signs a false message to shift the blame to other ring members.

It is well-known that group signature [4–9] can prevent its members from abusing anonymity, in which users are able to sign messages anonymously, but, when a dispute occurs, the group manager possessing a group master secret key is capable of revoking the anonymity of misbehaving signers. However, group signature cannot handle the leaking secrets scenario, as the the manager is always able to trace the real signer who leaks a piece of invaluable information. Besides, group signature has much higher costs on managing a dynamic group. Finally, the members are anxious that their anonymity will be or has been violated by the manager without notification.

In 2006, Komano et al. [10] formalized the notion of Deniable Ring Signature (DRS), which is as flexible as the ring signature and allows the members to confirm whether they are the real signer or not. Specifically, by using an interactive mechanism between the ring member and the verifier, it enables the real signer to confirm its signed action and allows other ring members to deny their involvement. In short, DRS can be regarded as a 'lightweight' group signature, i.e., group signature without the manager. For the security requirements, the DRS should satisfy:

- *Anonymity*: Any adversary should not get any information from the signature, unless the ring members are required to confirm or disavow their involvement in the signature.
- *Traceability*: Any adversary should not generate a valid ring signature such that no member will be detected as the real signer via the confirmation/disavowal protocol. In other words, the real singer cannot deny its signature.
- *Non-frameability*: Any adversary should not produce a valid ring signature such that a ring member, whose secret key is unknown to the adversary, will be detected as the real signer via the confirmation/disavowal protocol. In other words, any adversary cannot frame an honest member.

In their pioneering work, Komano et al. [10] also presented a concrete scheme under the Decisional Diffie–Hellman (DDH) assumption. However, this assumption does not hold in the quantum world [11].

1.1. Contributions and Technical Overview

In this work, we propose an efficient lattice-based *Non-interactive* Deniable Ring Signature (NDRS) scheme. The notion NDRS, first formalized in Reference [12], means that the confirmation or disavowal of a signature is achieved in a non-interactive manner, instead of the interactive mechanism between the ring member and the verifier. In terms of effiency, our construction is efficient in the sense that the signature size is only logarithmic to the cardinality of the ring. In the aspect of security, our construction satisfies the anonymity, traceability, and non-frameability under the Small Integer Solution (SIS) assumption in the random oracle model.

From a high level, our scheme is a natural extension of the ring signature scheme in Reference [8] to the NDRS setting. In more detail, we adapt their argument system for a tree-based accumulator [8] to allow the prover to convince the verifier that the prover knows a witness which *not only* accumulates to the root of a Merkle tree *but also* satisfies some additional conditions. Specifically, compared with the ring signature scheme in Reference [8], we add one more additional condition, an non-interactive identification scheme used by the ring members to prove their identity. Combining zero-knowledge argument systems for two or more NP relations is a general strategy widely used in previous works, such as group signatures [8,9], policy-based signatures [13], compact e-cash [14], etc.

The starting point of our construction is the Zero Knowledge Argument of Knowledge (ZKAoK) for the Merkle tree-based accumulator [8]. Specifically, the underlying hash function is defined by $h_{\mathbf{A}}(\mathbf{x}) = \mathsf{bin}(\mathbf{A} \cdot \mathbf{x} \bmod q) \in \{0,1\}^{m/2}$, where the uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ serves as the common reference string, $\mathbf{x} \in \{0,1\}^m$ is the input vector, and $\mathsf{bin}(\cdot)$ denotes the coordinate-wise binary decomposition of its input. Then, by using the framework of Stern's protocol [15], Libert et al. [8] can prove knowledge of hash chain in a zero-knowledge fashion. Besides, through the Fait-Shamir transformation, they also build ring signature with logarithmic size in the number of ring. Note that their ring signature enjoys complete anonymity. To achieve our goal that each ring member is able to generate a piece of evidence demonstrating whether it is the real signer or not, we need another matrix $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$ which acts as the public key of an identification scheme. In more detail, to sign a message M, a signer possessing his secret $\mathbf{x}$ generates a zero-knowledge argument system to show that:

Fact 1 $\mathbf{d} = h_{\mathbf{A}}(\mathbf{x})$.

Fact 2 $\mathbf{d}$ is properly accumulated into the root of the Merkle tree.

Fact 3 $\mathbf{B} \cdot \mathbf{x} = \mathbf{b} \bmod q$.

We first use the procedure in Reference [8] as a sub-protocol to prove Fact 1 and Fact 2 in zero knowledge. The key point in our construction is to prove the secret in Fact 1 *simultaneously* satisfies Fact 3. To this end, we employ again the framework of Stern's

protocol [15] as a sub-protocol, such that it is compatible with the proof in Reference [8]. The details are presented in Section 3.

Then, we apply the Fait-Shamir transformation to our interactive protocol and obtain a signature scheme in the random oracle by repeating it $\kappa = \omega(\log n)$ times to make the soundness error negligibly small. Generally, the anonymity of our NDRS scheme is based on the zero-knowledge property of the underlying argument system, while the traceability and the non-frameability are built on the fact that the underlying argument system is indeed an argument of knowledge. The description of the construction and its proof are described in Section 4.

1.2. Related Works

In 2006, Komano et al. [10] first introduced the notion of DRS and proposed a concrete DRS construction based on the DDH assumption. Recently, Gao et al. [12] put forward the NDRS notion, which is a direct generalization of DRS to the non-interactive setting. Besides, they proposed a concrete NDRS scheme under lattice assumptions, which is conjectured resistance against quantum computers. Their scheme, however, is shown to be insecure in Reference [16], as the scheme does not meet the 'Traceability' and 'Non-frameability' security requirements.

1.3. Organizations

We start in Section 2 by providing some background regarding NDRS and useful tools developed in Reference [8]. Then, in Section 3, we present an interactive protocol, which is the key component of our construction. In Section 4, we show the concrete scheme and its efficiency analysis and security proof. Finally, we conclude the paper with the obtained results.

2. Preliminaries

The set of integers $\{1, \ldots, k\}$ is denoted by $[k]$. If S is a finite set, $x \leftarrow S$ means that x is chosen uniformly at random from S. For $b \in \{0,1\}$, let $\bar{b} = 1 - b$. $\oplus$ denotes the bit XOR operation. For any positive integer q, denote by $\mathbb{Z}_q$ the quotient ring $\mathbb{Z}/(q\mathbb{Z})$. Vectors, denoted by bold lowercase letters, are in column form. Matrices are represented in bold uppercase letters, and the concatenation of two matrices, say $\mathbf{A} \in \mathbb{Z}_q^{n \times m_1}$ and $\mathbf{B} \in \mathbb{Z}_q^{n \times m_2}$, is denoted by $[\mathbf{A} \mid \mathbf{B}] \in \mathbb{Z}_q^{n \times (m_1 + m_2)}$. The tensor product is denoted by $\otimes$. Let B_{2m}^m be the set of all vectors in $\{0,1\}^{2m}$ with Hamming weight m, and $\mathcal{S}_{2m}$ be the set of all permutations of $2m$ elements. The abbreviation PPT means "probabilistic polynomial time".

Throughout the paper, we denote by n the security parameter and define: $q = \widetilde{O}(n)$; $k = \lceil \log q \rceil$; $m = 2nk$. Let $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g}^t \in \mathbb{Z}_q^{n \times nk}$, where $\mathbf{g}^t$ is the row vector

$$\mathbf{g}^t = [1\ 2\ 4\ \cdots\ 2^{k-1}] \in \mathbb{Z}_q^{1 \times k}.$$

Note that, for any $\mathbf{v} \in \mathbb{Z}_q^n$, we have $\mathbf{v} = \mathbf{G} \cdot \mathsf{bin}(\mathbf{v})$, where $\mathsf{bin}(\mathbf{v}) \in \{0,1\}^{nk}$ denotes the binary representation of $\mathbf{v}$.

2.1. Non-Interactive Deniable Ring Signature (NDRS)

For any positive integer $N \geq 2$, the ring R, formed by N users' public keys, is denoted by $R = \{pk_{i_0}, pk_{i_1}, \ldots, pk_{i_{N-1}}\}$. For ease of notation, we simply let $R = \{pk_0, pk_1, \ldots, pk_{N-1}\}$ with ring size N. Now, we recall the definition and security requirements for the NDRS presented in Reference [12].

- $\mathsf{Setup}(1^n)$: Take as input n and output the system parameter pp.
- $\mathsf{KeyGen}(\mathsf{pp})$: Take as input pp and output a public/secret key pair (pk, sk).
- $\mathsf{Sign}(\mathsf{pp}, R, sk, M)$: Take as inputs pp, a set of N public keys $R = \{pk_0, pk_1, \ldots, pk_{N-1}\}$, a secret key sk for which its corresponding $pk \in R$ and a message M to be signed, and output a ring signature Σ.

- $\mathsf{Verify}(\mathsf{pp}, R, M, \Sigma)$: Take as inputs pp, R, M, and Σ, and output 1 if Σ is valid or 0 otherwise.
- $\mathsf{EvidenceGen}(\mathsf{pp}, R, sk_i, \Sigma)$: Take as inputs pp, R, user i's secret key sk_i, M, and Σ, and output a piece of evidence ξ_i.
- $\mathsf{EvidenckCheck}(\mathsf{pp}, R, i, \xi_i, \Sigma)$: Take as inputs pp, R, an identity index i of a user, M and Σ, and output "confirmation", "disavowal", or "reject".

The correctness requirements for an NDRS scheme are formalized as follows:

1. The signature Σ generated by the Sign algorithm is properly accepted by the Verify algorithm, i.e., $\mathsf{Verify}(\mathsf{pp}, R, M, \Sigma) = 1$ for any $\mathsf{pp} \leftarrow \mathsf{Setup}(1^n)$, any $(pk, sk) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$, any R such that $pk \in R$ and any $M \in \{0,1\}^*$.
2. The real signer of the signature Σ will generate a piece of evidence such that the evidence check algorithm outputs "confirmation", i.e.,

$$\mathsf{EvidenckCheck}\big(\mathsf{pp}, R, i, \mathsf{EvidenceGen}(\mathsf{pp}, R, sk_i, \Sigma), \Sigma\big) = \text{"confirmation"}$$

   for any valid signature Σ generated by user i.
3. The non-real signer should generate a piece of evidence such that the evidence check algorithm outputs "disavowal", i.e.,

$$\mathsf{EvidenceCheck}\big(\mathsf{pp}, R, j, \mathsf{EvidenceGen}(\mathsf{pp}, R, sk_j, \Sigma), \Sigma\big) = \text{"disavowal"}$$

   for any ring member $j \neq i$.

For the security requirements, we adopt the notions and games in References [10,12]. Suppose each user has a public/private key pair supported by the Public Key Infrastructure (PKI). Let List be a public key content issued by PKI, and let MList be a list of malicious signers. Let GSet be a list of message-signature pairs generated through a challenge oracle query $\mathsf{Ch}_b(\cdot)$. An adversary is able to make the following queries.

- $\mathsf{Add}(i)$: on input i, this oracle generates a key pair (pk_i, sk_i) for user i, adds i together with the key pair to List, and returns pk_i.
- $\mathsf{Reg}(i, pk_i)$: on inputs i and pk_i, this oracle registers a new signer i with the given public key pk_i in List and adds user i to MList.
- $\mathsf{Crpt}(i)$: on input i, this oracle returns the secret key sk_i and adds user i to MList.
- $\mathsf{DRSig}(i_k; M, i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_t)$: on inputs a specified user i_k, a message M, and a set of identities, this oracle returns a signature Σ associated with the ring formed by the input identities, by using the secret key of user i_k.
- $\mathsf{Ch}_b(i_0, i_1, M)$: on inputs a pair of identities (i_0, i_1) and M, this oracle returns the signature $\mathsf{Sign}(\mathsf{pp}, \{pk_{i_0}, pk_{i_1}\}, sk_{i_b}, M)$ for a challenge bit $b \leftarrow \{0,1\}$, and adds it to GSet. This oracle is only used in the definition of anonymity.
- $\mathsf{EGen}(i, M, \Sigma)$: on inputs i, M, Σ, this oracle returns a piece of evidence demonstrating whether the entity i is the real signer or not. This oracle will reject the query if the input signature is an output from the challenge oracle in the experiment of anonymity.
- $\mathsf{Hash}(\cdot)$: this oracle outputs a random string with a fixed length for an arbitrary input.

As mentioned before, an (N)DRS scheme should satisfy anonymity, traceability, and non-frameability. Each of these security requirements is formalized by an experiment, as shown in Figure 1.

Anonymity

For an NDRS scheme, a security parameter n, and a PPT adversary $\mathcal{A}$, the property of anonymity is formalized using the experiment $\mathbf{Exp}^{\mathsf{anon}-b}_{NDRS,\mathcal{A}}(n)$, as described in Figure 1. The advantage $\mathbf{Adv}^{\mathsf{anon}}_{NDRS,\mathcal{A}}(n)$ is defined as

$$\mathbf{Adv}^{\mathsf{anon}}_{NDRS,\mathcal{A}}(n) = \Big|2\Pr[\mathbf{Exp}^{\mathsf{anon}-b}_{NDRS,\mathcal{A}}(n) = b] - 1\Big|.$$

An NDRS has anonymity if $\mathbf{Adv}^{\mathsf{anon}-b}_{NDRS,\mathcal{A}}(n)$ is negligible for any PPT adversary $\mathcal{A}$ and security parameter n.

- Experiment $\mathbf{Exp}^{\mathsf{anon}-b}_{NDRS,\mathcal{A}}(n)$
  $\mathsf{List} \leftarrow \emptyset$; $\mathsf{MList} \leftarrow \emptyset$; $\mathsf{GSet} \leftarrow \emptyset$;
  $b' \leftarrow \mathcal{A}(\mathsf{Add}(\cdot), \mathsf{Reg}(\cdot), \mathsf{Crpt}(\cdot), \mathsf{Ch}_b(\cdot), \mathsf{DRSig}(\cdot), \mathsf{EGen}(\cdot))$;
  If $i \in \mathsf{GSet}$ and $i \in \mathsf{MList}$ Then return 0 Else return b'
- Experiment $\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$
  $\mathsf{List} \leftarrow \emptyset$; $\mathsf{MList} \leftarrow \emptyset$; $\mathsf{GSet} \leftarrow \emptyset$;
  $(M, \Sigma, \{pk_{i_1}, \ldots, pk_{i_t}\}) \leftarrow \mathcal{A}(\mathsf{Add}(\cdot), \mathsf{Reg}(\cdot), \mathsf{Crpt}(\cdot), \mathsf{DRSig}(\cdot), \mathsf{EGen}(\cdot))$;
  If $\mathsf{Verify}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, M, \Sigma) = 0$ Then return 0;
  $\xi_{i_k} \leftarrow \mathsf{EvidenceGen}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, sk_{i_k}, M, \Sigma)$;
  If $\forall\, i_j \in i_1, \ldots, i_N$
  $\mathsf{EvidenceCheck}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, i_j, \xi_{i_k}, M, \Sigma) = 0$
  Then return 1 Else return 0
- Experiment $\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$
  $\mathsf{List} \leftarrow \emptyset$; $\mathsf{MList} \leftarrow \emptyset$; $\mathsf{GSet} \leftarrow \emptyset$;
  $(M, \Sigma, \{pk_{i_1}, \ldots, pk_{i_t}\}) \leftarrow \mathcal{A}(\mathsf{Add}(\cdot), \mathsf{Reg}(\cdot), \mathsf{Crpt}(\cdot), \mathsf{DRSig}(\cdot), \mathsf{EGen}(\cdot))$
  If $\mathsf{Verify}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, M, \Sigma) = 0$ Then return 0
  If the following two conditions are satisfied Then return 1
  Else return 0
  - For some $k \in [t]$,
    $\xi_{i_k} = \mathsf{EvidenceGen}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, sk_{i_k}, M, \Sigma)$,
    $\mathsf{EvidenceCheck}(\mathsf{pp}, \{pk_{i_1}, \ldots, pk_{i_t}\}, i_k, \xi_{i_k}, M, \Sigma) =$"confirmation"
  - $\mathcal{A}$ did not query $\mathsf{DRSig}(i_k; M, i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_t)$, $\mathsf{Reg}(i_k)$ or $\mathsf{Crpt}(i_k)$

Figure 1. Experiments of anonymity, traceability, and non-frameability.

Traceability

The property of traceability is formalized using the experiment $\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$, as shown in Figure 1. The advantage of the adversary is given by:

$$\mathbf{Adv}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n) = \Pr[\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n) = 1].$$

An NDRS is said to hold traceability if $\mathbf{Adv}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$ is negligible for any PPT adversary $\mathcal{A}$ and security parameter n.

Non-frameability

The property of non-frameability is formalized using the experiment $\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$, as shown in Figure 1. The advantage of the adversary is defined as:

$$\mathbf{Adv}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n) = \Pr[\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n) = 1].$$

An NDRS is said to hold non-frameability if $\mathbf{Adv}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$ is negligible for any PPT adversary $\mathcal{A}$ and security parameter n.

2.2. Average-Case Lattice Problems

In this subsection, we briefly recall the average-case Small Integer Soulution (SIS) problem (in the infinity norm version) and its hardness guarantees. For more details, see References [17–20].

Definition 1 (Reference [17])**.** *Given uniformly random matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$*, the* $\mathsf{SIS}^{\infty}_{n,m,q,\beta}$ *problem asks to find a non-zero vector* $\mathbf{x} \in \mathbb{Z}^m$ *such that* $\mathbf{A} \cdot \mathbf{x} = \mathbf{0} \bmod q$ *and* $\|\mathbf{x}\|_\infty \leq \beta$*.*

The hardness of the SIS problem is guaranteed by a certain lattice problems in the worst case, such as the Shortest Independent Vector Problem (SIVP).

Theorem 1 (References [18–20]). *If* $m, \beta = \mathsf{poly}(n)$, *and* $q > \beta \cdot \widetilde{O}(\sqrt{n})$, *then the* $\mathsf{SIS}^{\infty}_{n,m,q,\beta}$ *problem is at least as hard as the worst-case problem* SIVP_{γ} *for some* $\gamma = \beta \cdot \widetilde{O}(\sqrt{mn})$. *Specifically, for* $\beta = 1, q = \widetilde{O}(n), m = 2n\lceil \log q \rceil$, *the* $\mathsf{SIS}^{\infty}_{n,m,q,1}$ *problem is at least as hard as* $\mathsf{SIVP}_{\widetilde{O}(n)}$.

2.3. Statistical Zero-Knowledge Argument Systems

Let $R : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ be an NP relation. The interaction $\langle \mathcal{P}, \mathcal{V} \rangle$ between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$ is called an interactive argument system for the relation R if the following two conditions hold:

Completeness

If $R(x,w) = 1$, then

$$\Pr[\langle \mathcal{P}(x,w), \mathcal{V}(x) \rangle = 1] = 1.$$

Soundness

If $R(x,w) = 0$, then, for every PPT $\mathcal{P}^*$:

$$\Pr[\langle \mathcal{P}^*(x,w), V(x) \rangle = 1] \leq e,$$

where $e \in [0,1]$ is called the soundness error.

In this work, we will employ the Stern-type ZKAoK [15], which is a Σ-protocol from a generalized point of view in References [21,22]. Besides, we will utilize the lattice-based string commitment scheme in Reference [23] $\mathsf{COM} : \{0,1\}^* \times \{0,1\}^{m/2} \to \mathbb{Z}_q^n$, which is statistically hiding and computationally binding under the assumption that $\mathsf{SIVP}_{\widetilde{O}(n)}$ is hard.

2.4. Lattice-Based Accumulator

We first recall a certain family of collision-resistant hash functions presented in Reference [8].

Definition 2. *The function family* $\mathcal{H} : \{0,1\}^{nk} \times \{0,1\}^{nk} \to \{0,1\}^{nk}$ *is given by* $\mathcal{H} = \{h_{\mathbf{A}} : \mathbf{A} \in \mathbb{Z}_q^{n \times m}\}$, *where*

$$h_{\mathbf{A}}(\mathbf{u}_0, \mathbf{u}_1) = \mathsf{bin}(\mathbf{A}_0 \cdot \mathbf{u}_0 + \mathbf{A}_1 \cdot \mathbf{u}_1 \mod q) \in \{0,1\}^{nk}.$$

for any $(\mathbf{u}_0, \mathbf{u}_1) \in \{0,1\}^{nk} \times \{0,1\}^{nk}$, *and* $\mathbf{A} = [\mathbf{A}_0 \mid \mathbf{A}_1]$ *with* $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_q^{n \times nk}$.

Then, we recall the Merkle tree accumulator with $N = 2^l$ leaves based on the hash function family $\mathcal{H}$ above.

- $\mathsf{TSetup}(1^n)$: On input n, output $\mathsf{pp} = \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$.
- $\mathsf{TAcc}(\mathbf{A}, R\})$: Given $R = \{\mathbf{d}_j \in \{0,1\}^{nk}\}_{j=0}^{N-1}$, let $\mathbf{u}_{j_1,\ldots,j_l} = \mathbf{d}_j$, where $j_1, \ldots, j_l \in \{0,1\}$ is the l bits of j. Define the tree of depth l for the leaves $\mathbf{u}_{0,\ldots,0}, \ldots, \mathbf{u}_{1,\ldots,1}$ as follows:
  1. The nodes $\mathbf{u}_{b_1,\ldots,b_i}$ at depth $i \in [l]$ is given by $h_{\mathbf{A}}(\mathbf{u}_{b_1,\ldots,b_i,0}, \mathbf{u}_{b_1,\ldots,b_i,1})$.
  2. The root $\mathbf{u} \in \{0,1\}^{nk}$ is defined as $h_{\mathbf{A}}(\mathbf{u}_0, \mathbf{u}_1)$.

  Output $\mathbf{u}$ as the accumulator value.
- $\mathsf{TWitness}(\mathbf{A}, R, \mathbf{d})$: If $\mathbf{d} \notin R$, output $\perp$; otherwise, $\exists\, j \in [0, N-1]$ such that $\mathbf{d} = \mathbf{d}_j$. Return the witness w defined by:

$$w = \left((j_1, \ldots, j_l), (\mathbf{u}_{j_1,\ldots,j_{l-1},\bar{j_l}}, \ldots, \mathbf{u}_{j_1,\bar{j_2}}, \mathbf{u}_{\bar{j_1}})\right) \in \{0,1\}^l \times (\{0,1\}^{nk})^l,$$

  where $\mathbf{u}_{j_1,\ldots,j_{l-1},\bar{j_l}}, \ldots, \mathbf{u}_{j_1,\bar{j_2}}, \mathbf{u}_{\bar{j_1}}$ are computed by $\mathsf{TAcc}(\mathbf{A}, R)$.
- $\mathsf{TVerify}(\mathbf{A}, \mathbf{u}, \mathbf{d}, w)$: Given witness

$$w = \big((j_1, \ldots, j_l), (\mathbf{w}_l, \ldots, \mathbf{w}_1)\big) \in \{0,1\}^l \times (\{0,1\}^{nk})^l,$$

let $\mathbf{v}_l = \mathbf{d}$, and recursively compute $\mathbf{v}_{l-1}, \ldots, \mathbf{v}_1, \mathbf{v}_0 \in \{0,1\}^{nk}$ for $i \in \{l-1, \ldots, 0\}$ as follows:

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

Return 1 if $\mathbf{v}_0 = \mathbf{u}$; otherwise, return 0.

In Reference [8], the authors also design an argument system for the prover $\mathcal{P}$ to convince the verifier $\mathcal{V}$ that $\mathcal{P}$ knows a value-witness pair $(\mathbf{d}, w)$ such that $\mathsf{TVerify}(\mathbf{A}, \mathbf{u}, \mathbf{d}, w) = 1$. Toward this goal, they develop the following supporting techniques, which are necessary in our construction, as well.

- Extension of $\mathbf{A} = [\mathbf{A}_0 \mid \mathbf{A}_1]$ to $\mathbf{A}^* = [\mathbf{A}_0 \mid \mathbf{0}^{n \times nk} \mid \mathbf{A}_1 \mid \mathbf{0}^{n \times nk}] \in \mathbb{Z}_q^{n \times 2m}$.
- Extension of $\mathbf{G}$ to $\mathbf{G}^* = [\mathbf{G} \mid \mathbf{0}^{n \times nk}] \in \mathbb{Z}_q^{n \times m}$.
- Extensions of $\mathbf{v}_1, \ldots, \mathbf{v}_l, \mathbf{w}_1, \ldots, \mathbf{w}_l$ to $\mathbf{v}_1^*, \ldots, \mathbf{v}_l^*, \mathbf{w}_1^*, \ldots, \mathbf{w}_l^* \in \mathsf{B}_m^{nk}$ by appending to each vector a length-nk vector with suitable Hamming weight.
- For $i \in \{nk, m\}, b \in \{0,1\}$ and $\mathbf{v} \in \{0,1\}^i$, let $\mathsf{ext}(b, \mathbf{v})$ denote the vector $\mathbf{z} \in \{0,1\}^{2i}$ of the form $\mathbf{z} = \begin{pmatrix} \bar{b} \cdot \mathbf{v} \\ b \cdot \mathbf{v} \end{pmatrix}$.
- For $b \in \{0,1\}$ and $\pi \in \mathcal{S}_m$, define the permutation $F_{b,\pi}$ that transforms $\mathbf{z} = \begin{pmatrix} \mathbf{z}_0 \\ \mathbf{z}_1 \end{pmatrix} \in \mathbb{Z}_q^{2m}$ consisting of 2 blocks of size m into $F_{b,\pi}(\mathbf{z}) = \begin{pmatrix} \pi(\mathbf{z}_b) \\ \pi(\mathbf{z}_{\bar{b}}) \end{pmatrix}$.

Observe that, for all $c, b \in \{0,1\}, \pi, \phi \in \mathcal{S}_m$ and $\mathbf{v}, \mathbf{w} \in \{0,1\}^m$,

$$\mathbf{z} = \mathsf{ext}(c, \mathbf{v}) \wedge \mathbf{v} \in \mathsf{B}_m^{nk} \iff F_{b,\pi}(\mathbf{z}) = \mathsf{ext}(c \oplus b, \pi(\mathbf{v})) \wedge \pi(\mathbf{v}) \in \mathsf{B}_m^{nk};$$
$$\mathbf{y} = \mathsf{ext}(\bar{c}, \mathbf{w}) \wedge \mathbf{w} \in \mathsf{B}_m^{nk} \iff F_{\bar{b},\phi}(\mathbf{y}) = \mathsf{ext}(c \oplus b, \phi(\mathbf{w})) \wedge \phi(\mathbf{w}) \in \mathsf{B}_m^{nk}.$$

3. The Underlying Zero-Knowledge Argument System

In this section, we present an interactive protocol, upon which our NDRS scheme is built. This protocol bears much resemblance to that in Section 4.2 of Reference [8], except that one more layer is added. Specifically, in our protocol, the prover $\mathcal{P}$ is able to convince the verifier $\mathcal{V}$ on input $(\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b})$ that $\mathcal{P}$ knows a secret tuple $(\mathbf{d}, w, \mathbf{x})$ such that:

- $\mathbf{d} = h_{\mathbf{A}}(\mathbf{x}) \in \{0,1\}^{nk}$,
- $\mathsf{TVerify}(\mathbf{A}, \mathbf{u}, \mathbf{d}, w) = 1$,
- $\mathbf{B} \cdot \mathbf{x} = \mathbf{b} \bmod q \in \mathbb{Z}_q^n$.

More formally, the associated relation $\mathrm{R}_{\mathrm{NDRS}}$ is given by

$$\begin{aligned} \mathrm{R}_{\mathrm{NDRS}} = \big\{ \big((\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{n \times m} \times \{0,1\}^{nk} \times \mathbb{Z}_q^n; \\ \mathbf{d} \in \{0,1\}^{nk}, w \in \{0,1\}^l \times (\{0,1\}^{nk})^l, \mathbf{x} \in \{0,1\}^m \big) : \\ \mathbf{A} \cdot \mathbf{x} = \mathbf{G} \cdot \mathbf{d} \mod q \ \wedge \ \mathbf{B} \cdot \mathbf{x} = \mathbf{b} \mod q \ \wedge \ \mathsf{TVerify}(\mathbf{A}, \mathbf{u}, \mathbf{d}, w) = 1 \big\}. \end{aligned}$$

3.1. Description of the Interactive Protocol

The public parameters are $n, m, q, k, l, \mathbf{G}, \mathbf{G}^*, \hat{\mathbf{A}}$, and $\hat{\mathbf{B}}$, where

$$\hat{\mathbf{A}} = [\mathbf{A} \mid \mathbf{0}^{n \times m}], \hat{\mathbf{B}} = [\mathbf{B} \mid \mathbf{0}^{n \times m}] \in \mathbb{Z}_q^{n \times 2m}.$$

The prover $\mathcal{P}$, using its witness, prepares, according to Section 2.4, the following vectors:

$$\mathbf{v}_i^*, \ \mathbf{w}_i^* \in \mathsf{B}_m^{nk}, \ \ \mathbf{z}_i = \mathsf{ext}(j_i, \mathbf{v}_i^*), \ \ \mathbf{y}_i = \mathsf{ext}(\bar{j}_i, \mathbf{w}_i^*),$$

for all $i \in [l]$ such that

$$\begin{cases} \mathbf{A}^* \cdot \mathbf{z}_1 + \mathbf{A}^* \cdot \mathbf{y}_1 = \mathbf{G} \cdot \mathbf{u} \mod q; \\ \mathbf{A}^* \cdot \mathbf{z}_{i+1} + \mathbf{A}^* \cdot \mathbf{y}_{i+1} = \mathbf{G}^* \cdot \mathbf{v}_i^* \mod q \end{cases}, \tag{1}$$

for all $i \in [l-1]$. Observe that $\mathbf{G}^* \cdot \mathbf{v}_l^* = \mathbf{G} \cdot \mathbf{d}$. First, $\mathcal{P}$ extends $\mathbf{x}$ into $\mathbf{x}^* \in \mathsf{B}_{2m}^m$. Clearly, $\hat{\mathbf{A}} \cdot \mathbf{x}^* = \mathbf{A} \cdot \mathbf{x}$ and $\hat{\mathbf{B}} \cdot \mathbf{x}^* = \mathbf{B} \cdot \mathbf{x}$. In Stern's framework, a random permutation $\tau \leftarrow \mathcal{S}_{2m}$ and a random 'mask' $\mathbf{r}_\mathbf{x} \leftarrow \mathbb{Z}_q^{2m}$ give a ZKAoK of the secret $\mathbf{x}$ according to the equivalence $\mathbf{x}^* \in \mathsf{B}_{2m}^m \Leftrightarrow \tau(\mathbf{x}^*) \in \mathsf{B}_{2m}^m$.

After these preparations, $\mathcal{P}$'s goal is to convince $\mathcal{V}$ that it knows the vectors $\mathbf{v}_i^*,\ \mathbf{w}_i^*$, $\mathbf{z}_i,\ \mathbf{y}_i$ for all $i \in [l]$ and $\mathbf{x}^* \in \mathsf{B}_{2m}$ such that:

- Equation (1) holds;
- $\hat{\mathbf{A}} \cdot \mathbf{x}^* = \mathbf{G}^* \cdot \mathbf{v}_l^* \mod q$ and $\hat{\mathbf{B}} \cdot \mathbf{x}^* = \mathbf{b} \mod q$.

The interaction between $\mathcal{P}$ and $\mathcal{V}$ is detailed as follows.

1. **Commitment.** $\mathcal{P}$ firstly picks the following randomness:

$$\begin{gathered} \rho_1, \rho_2, \rho_3 \in \{0,1\}^{m/2} \text{ for } \mathsf{COM} \\ \tau \leftarrow \mathcal{S}_{2m};\ b_1, \ldots, b_l \leftarrow \{0,1\};\ \pi_1, \ldots, \pi_l,\ \phi_1, \ldots, \phi_l \leftarrow \mathcal{S}_m \\ \mathbf{r}_\mathbf{x} \leftarrow \mathbb{Z}_q^{2m};\ \mathbf{r}_{\mathbf{v}_1}, \ldots, \mathbf{r}_{\mathbf{v}_l} \leftarrow \mathbb{Z}_q^m;\ \mathbf{r}_{\mathbf{z}_1}, \ldots, \mathbf{r}_{\mathbf{z}_l},\ \mathbf{r}_{\mathbf{y}_1}, \ldots, \mathbf{r}_{\mathbf{y}_l} \leftarrow \mathbb{Z}_q^{2m}. \end{gathered}$$

Then, the commitment CMT=(C_1, C_2, C_3) is sent to $\mathcal{V}$, where

$$\begin{aligned} C_1 &= \mathsf{COM}\big(\tau;\ \hat{\mathbf{A}} \cdot \mathbf{r}_\mathbf{x} - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_l};\ \hat{\mathbf{B}} \cdot \mathbf{r}_\mathbf{x};\ \{b_i, \pi_i, \phi_i\}_{i=1}^l;\ \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_1} + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_1}; \\ &\qquad \{\mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_{i+1}} + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_{i+1}} - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_i}\}_{i=1}^{l-1};\ \rho_1\big) \\ C_2 &= \mathsf{COM}\big(\tau(\mathbf{r}_\mathbf{x});\ \{\pi_i(\mathbf{r}_{\mathbf{v}_i}), F_{b_i,\pi_i}(\mathbf{r}_{\mathbf{z}_i}), F_{\bar{b}_i,\phi_i}(\mathbf{r}_{\mathbf{y}_i})\}_{i=1}^l;\ \rho_2\big) \\ C_3 &= \mathsf{COM}\big(\tau(\mathbf{x}^* + \mathbf{r}_\mathbf{x});\ \{\pi_i(\mathbf{v}_i^* + \mathbf{r}_{\mathbf{v}_i}), F_{b_i,\pi_i}(\mathbf{z}_i + \mathbf{r}_{\mathbf{z}_i}), F_{\bar{b}_i,\phi_i}(\mathbf{y}_i + \mathbf{r}_{\mathbf{y}_i})\}_{i=1}^l;\ \rho_3\big). \end{aligned}$$

2. **Challenge.** $\mathcal{V}$ sends to $\mathcal{P}$ a challenge $Ch \leftarrow \{1,2,3\}$.
3. **Response.** $\mathcal{P}$ sends the response RSP depending on Ch as follows:

- $Ch = 1$: Let $\widetilde{\mathbf{x}}^* = \tau(\mathbf{x}^*), \widetilde{\mathbf{r}}_\mathbf{x} = \tau(\mathbf{r}_\mathbf{x})$, and, for each $i \in [l]$, let:

$$\begin{gathered} \widetilde{b}_i = j_i \oplus b_i;\ \widetilde{\mathbf{v}}_i^* = \pi_i(\mathbf{v}_i^*);\ \widetilde{\mathbf{w}}_i^* = \phi_i(\mathbf{w}_i^*) \\ \widetilde{\mathbf{r}}_{\mathbf{v}_i} = \pi_i(\mathbf{r}_{\mathbf{v}_i});\ \widetilde{\mathbf{r}}_{\mathbf{z}_i} = F_{b_i,\pi_i}(\mathbf{r}_{\mathbf{z}_i});\ \widetilde{\mathbf{r}}_{\mathbf{y}_i} = F_{\bar{b}_i,\phi_i}(\mathbf{r}_{\mathbf{y}_i}). \end{gathered}$$

  Set RSP=$\big(\widetilde{\mathbf{x}}^*;\ \widetilde{\mathbf{r}}_\mathbf{x};\ \{\widetilde{b}_i, \widetilde{\mathbf{v}}_i^*, \widetilde{\mathbf{w}}_i^*, \widetilde{\mathbf{r}}_{\mathbf{v}_i}, \widetilde{\mathbf{r}}_{\mathbf{z}_i}, \widetilde{\mathbf{r}}_{\mathbf{y}_i}\}_{i=1}^l;\ \rho_2;\ \rho_3\big)$.
- $Ch = 2$: Let $\tau' = \tau,\ \mathbf{s}_\mathbf{x} = \mathbf{x}^* + \mathbf{r}_\mathbf{x}$, and, for each $i \in [l]$, let:

$$\begin{gathered} b_i' = b_i;\ \pi_i' = \pi_i;\ \phi_i' = \phi_i; \\ \mathbf{s}_{\mathbf{v}_i} = \mathbf{v}_i^* + \mathbf{r}_{\mathbf{v}_i};\ \mathbf{s}_{\mathbf{z}_i} = \mathbf{z}_i + \mathbf{r}_{\mathbf{z}_i};\ \mathbf{s}_{\mathbf{y}_i} = \mathbf{y}_i + \mathbf{r}_{\mathbf{y}_i}. \end{gathered}$$

  Set RSP=$\big(\tau';\ \mathbf{s}_\mathbf{x};\ \{b_i', \pi_i', \phi_i', \mathbf{s}_{\mathbf{v}_i}, \mathbf{s}_{\mathbf{z}_i}, \mathbf{s}_{\mathbf{y}_i}\}_{i=1}^l;\ \rho_1;\ \rho_3\big)$.
- $Ch = 3$: Let $\tau'' = \tau,\ \mathbf{r}_\mathbf{x}' = \mathbf{r}_\mathbf{x}$, and, for each $i \in [l]$, let:

$$\begin{gathered} b_i'' = b_i;\ \pi_i'' = \pi_i;\ \phi_i'' = \phi_i; \\ \mathbf{r}_{\mathbf{v}_i}' = \mathbf{r}_{\mathbf{v}_i};\ \mathbf{r}_{\mathbf{z}_i}' = \mathbf{r}_{\mathbf{z}_i};\ \mathbf{r}_{\mathbf{y}_i}' = \mathbf{r}_{\mathbf{y}_i}. \end{gathered}$$

  Set RSP=$\big(\tau'';\ \mathbf{r}_\mathbf{x}';\ \{b_i'', \pi_i'',\ \phi_i'', \mathbf{r}_{\mathbf{v}_i}', \mathbf{r}_{\mathbf{z}_i}', \mathbf{r}_{\mathbf{y}_i}'\}_{i=1}^l;\ \rho_1;\ \rho_2\big)$.

4. **Verification.** Given RSP, $\mathcal{V}$ proceeds as follows.

- $Ch = 1$: Check that $\widetilde{\mathbf{x}}^* \in \mathsf{B}_{2m}$ for $i \in [p]$, $\widetilde{\mathbf{v}}_i^*, \widetilde{\mathbf{w}}_i^* \in \mathsf{B}_m^{nk}$ for $i \in [l]$ and that

$$C_2 = \mathsf{COM}\big(\widetilde{\mathbf{r}}_{\mathbf{x}};\ \{\widetilde{\mathbf{r}}_{\mathbf{v}_i}, \widetilde{\mathbf{r}}_{\mathbf{z}_i}, \widetilde{\mathbf{r}}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_2\big),$$
$$C_3 = \mathsf{COM}\big(\widetilde{\mathbf{x}}^* + \widetilde{\mathbf{r}}_{\mathbf{x}};\ \{\widetilde{\mathbf{v}}_i^* + \widetilde{\mathbf{r}}_{\mathbf{v}_i}, \mathsf{ext}(\widetilde{b}_i, \widetilde{\mathbf{v}}_i^*) + \widetilde{\mathbf{r}}_{\mathbf{z}_i}, \mathsf{ext}(\widetilde{b}_i, \widetilde{\mathbf{w}}_i^*) + \widetilde{\mathbf{r}}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_3\big).$$

- $Ch = 2$: Check that

$$C_1 = \mathsf{COM}\big(\tau';\ \hat{\mathbf{A}} \cdot \mathbf{s}_{\mathbf{x}} - \mathbf{G}^* \cdot \mathbf{s}_{\mathbf{v}_l};\ \hat{\mathbf{B}} \cdot \mathbf{s}_{\mathbf{x}} - \mathbf{b};\ \{b_i', \pi_i', \phi_i'\}_{i=1}^{l};$$
$$\mathbf{A}^* \cdot \mathbf{s}_{\mathbf{z}_1} + \mathbf{A}^* \cdot \mathbf{s}_{\mathbf{y}_1} - \mathbf{G} \cdot \mathbf{u}; \{\mathbf{A}^* \cdot \mathbf{s}_{\mathbf{z}_{i+1}} + \mathbf{A}^* \cdot \mathbf{s}_{\mathbf{y}_{i+1}} - \mathbf{G}^* \cdot \mathbf{s}_{\mathbf{v}_i}\}_{i=1}^{l-1};\ \rho_1\big),$$
$$C_3 = \mathsf{COM}\big(\tau'(\mathbf{s}_{\mathbf{x}});\ \{\pi_i'(\mathbf{s}_{\mathbf{v}_i}), F_{b_i', \pi_i'}(\mathbf{s}_{\mathbf{z}_i}), F_{\bar{b}_i', \phi_i'}(\mathbf{s}_{\mathbf{y}_i})\}_{i=1}^{l};\ \rho_3\big).$$

- $Ch = 3$: Check that

$$C_1 = \mathsf{COM}\big(\tau'';\ \hat{\mathbf{A}} \cdot \mathbf{r}_{\mathbf{x}}' - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_l}';\ \hat{\mathbf{B}} \cdot \mathbf{r}_{\mathbf{x}}';\ \{b_i'', \pi_i'', \phi_i''\}_{i=1}^{l};\ \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_1}' + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_1}';$$
$$\{\mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_{i+1}}' + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_{i+1}}' - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_i}'\}_{i=1}^{l-1};\ \rho_1\big),$$
$$C_2 = \mathsf{COM}\big(\tau''(\mathbf{r}_{\mathbf{x}}');\ \{\pi_i''(\mathbf{r}_{\mathbf{v}_i}'), F_{b_i'', \pi_i''}(\mathbf{r}_{\mathbf{z}_i}'), F_{\bar{b}_i'', \phi_i''}(\mathbf{r}_{\mathbf{y}_i}')\}_{i=1}^{l};\ \rho_2\big).$$

$\mathcal{V}$ outputs 1 only if all the conditions hold in each cases. Otherwise, output 0.

3.2. Analysis of the Interactive Protocol

We summarize several properties of the above protocol in the following theorem. Since the proof of the properties of the protocol is similar with that of Reference [8], we omit the details. (See Appendix A)

Theorem 2. *The given interactive protocol has perfect completeness and communication cost* $\widetilde{O}(l \cdot n)$. *If* COM *is a statistically hiding and computationally binding string commitment scheme, then it is an* ZKAoK *for the relation* $\mathrm{R}_{\mathrm{NDRS}}$.

4. Our Non-Interactive Deniable Ring Signature Scheme from Lattices

We now construct an NDRS scheme for rings with $N = 2^l$ users (It can be easily adapted for any other values of N as in Reference [8].) and prove that our construction satisfies the security requirements: anonymity, traceability, and non-frameability. We use a public Pseudo-random Generator (PRG), and a random oracle $\mathcal{H}_{\mathsf{FS}} : \{0,1\}^* \to \{1,2,3\}^{\kappa}$.

- $\mathsf{Setup}(1^n)$: On input n, output $\mathsf{pp} = \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$.
- $\mathsf{KeyGen}(\mathsf{pp})$: On input pp, output $(pk, sk) = (\mathbf{d}, \mathbf{x})$, where $\mathbf{x} \leftarrow \{0,1\}^m$, and $\mathbf{d} = \mathsf{bin}(\mathbf{A} \cdot \mathbf{x} \bmod q)$.
- $\mathsf{Sign}(\mathsf{pp}, R, sk, M)$: On inputs pp, $R = \{\mathbf{d}_0, \ldots, \mathbf{d}_{N-1}\}$, sk, and M, it works as follows (Notice that, for the public key pk corresponding to the input sk, we have $pk \in R$.) to output the signature Σ.

  1. Run $\mathsf{TAcc}(\mathbf{A}, R)$ and obtain $\mathbf{u} \in \{0,1\}^{nk}$. Recall that $\mathbf{u}$ is the root of the Merkle tree defined on R.
  2. Run $\mathsf{TWitness}(\mathbf{A}, R, \mathbf{d})$ and obtain

$$w = \big((j_1, \ldots, j_l) \in \{0,1\}^l, (\mathbf{w}_l \ldots, \mathbf{w}_1) \in (\{0,1\}^{nk})^l\big).$$

  Recall that w is a witness to the fact that $\mathbf{d} \in R$.
  3. Sample a seed $s \leftarrow \{0,1\}^n$, generate a matrix $\mathbf{B} = \mathsf{PRG}(s) \in \mathbb{Z}_q^{n \times m}$ and compute $\mathbf{b} = \mathbf{B} \cdot \mathbf{x} \bmod q$. Then, produce an $\mathsf{NIZKAoK}$ Π by repeating our interactive protocol $\kappa = \omega(\log n)$ times. By using the Fiat-Shamir heuristic, we transform Π to the triple

$$\Pi = \big(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}_i\}_{i=1}^{\kappa}\big),$$

where

$$\mathrm{CH} = \mathcal{H}_{\mathsf{FS}}\big(M, \{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}, R\big) = (Ch_1, \ldots, Ch_\kappa) \in \{1,2,3\}^\kappa.$$

4. Output $\Sigma = (s, \mathbf{b}, \Pi)$.

- $\mathsf{Verify}(\mathsf{pp}, R, M, \Sigma)$: Pm inputs $\mathsf{pp}, R, M, \Sigma$, the verification procedure is detailed as follows:
  1. Run $\mathsf{TAcc}(\mathbf{A}, R)$ and obtain $\mathbf{u}$.
  2. Parse $\Sigma = \big(s, \mathbf{b}, \{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}_i\}_{i=1}^{\kappa}\big)$. Let $\mathbf{B} = \mathsf{PRG}(s)$. Output 0 if
  $$(Ch_1, \ldots, Ch_\kappa) \neq \mathcal{H}_{\mathsf{FS}}\big(M, \{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}, R\big).$$
  3. For $i = 1, \ldots, \kappa$, check the validity of RSP_i *w.r.t.* CMT_i and Ch_i. If all the conditions hold, output 1; otherwise, output 0.
- $\mathsf{EvidenceGen}(\mathsf{pp}, R, sk_i, \Sigma)$: On inputs pp, R, a secret key $sk_i = \mathbf{x}'$, and the pair $(s, \mathbf{b})$ contained in Σ, the algorithm produces a piece of evidence ξ_i as follows:
  1. Run $\mathsf{TAcc}(\mathbf{A}, R)$ and obtain the Merkle tree's root $\mathbf{u} \in \{0,1\}^{nk}$.
  2. Let $pk_i = \mathbf{d}' = \mathsf{bin}(\mathbf{A} \cdot \mathbf{x}' \bmod q)$. Generate a witness
  $$w' = \big((j'_1, \ldots, j'_l) \in \{0,1\}^l, (\mathbf{w}'_l \ldots, \mathbf{w}'_1) \in (\{0,1\}^{nk})^l\big)$$
  to the fact that $\mathbf{d}' \in R$ by running $\mathsf{TWitness}(\mathbf{A}, R, \mathbf{d}')$, i.e., $\mathbf{d}'$ was properly accumulated in $\mathbf{u}$.
  3. Let $\mathbf{B} = \mathsf{PRG}(s)$. Compute $\mathbf{b}' = \mathbf{B} \cdot \mathbf{x}' \bmod q$ and generate a $\mathsf{NIZKAoK}$ Π' as in the signing algorithm to demonstrate the possession of a valid pair $(pk_i, sk_i) = (\mathbf{d}', \mathbf{x}')$ such that $\mathbf{b}' = \mathbf{B} \cdot \mathbf{x}' \bmod q$ and that $\mathbf{d}' \in R$, i.e.,
  $$\Pi' = \big(\{\mathrm{CMT'}_i\}_{i=1}^{\kappa}, \mathrm{CH}', \{\mathrm{RSP'}_i\}_{i=1}^{\kappa}\big),$$
  where
  $$\mathrm{CH}' = \mathcal{H}_{\mathsf{FS}}\big(\{\mathrm{CMT'}_i\}_{i=1}^{\kappa}, \mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}', R\big) \in \{1,2,3\}^\kappa.$$
  4. Output $\xi_i = (s, \mathbf{b}', \Pi')$. Note that ξ_i can be seen just as a signature on the empty message with the given seed s (instead of choosing a random seed by the algorithm itself).
- $\mathsf{EvidenceCheck}(\mathsf{pp}, R, i, \xi_i, \Sigma)$: On inputs $\mathsf{pp}, R, i, \xi_i, \Sigma$, the evidence ξ_i is checked as follows:
  1. Check the validity of ξ_i and Σ by verifying the underlying protocols. If either is invalid, then output "reject".
  2. If $(s, \mathbf{b}') = (s, \mathbf{b})$, then output "confirmation"; otherwise, output "disavowal".

Analysis of Our NDRS Scheme

We first briefly analyze the correctness and efficiency properties.

Theorem 3 (Correctness and Efficiency)**.** *The NDRS scheme described in the previous section is correct and produces signatures of bit-size* $\widetilde{O}(n \cdot \log N)$.

Correctness. It is easy to check that:

- By the perfect completeness of the argument system presented in the previous section, each member of a ring is always capable of obtaining a tuple $(\mathbf{x}, \mathbf{d}, w)$ such that
$$\big((\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}), \mathbf{d}, w, \mathbf{x}\big) \in \mathrm{R}_{\mathrm{NDRS}}.$$
Thus, by the Fiat-Shamir heuristic, the ring signature on M is valid.

- Meanwhile, for any signature $\Sigma = (s, \mathbf{b}, \Pi)$, the real signer can always produce a piece of valid evidence $\xi = (s, \mathbf{b}', \Pi')$ such that $\mathbf{b} = \mathbf{b}'$, i.e., EvidenceCheck outputs 'confirmation'.
- By the randomness of the secret keys $\mathbf{x}, \mathbf{x}' \leftarrow \{0,1\}^m$, the non-real signer can always produce a piece of valid evidence $\widetilde{\xi} = (s, \widetilde{\mathbf{b}}, \widetilde{\Pi})$ such that $\mathbf{b} = \mathbf{B} \cdot \mathbf{x} \mod q \neq \mathbf{b}' = \mathbf{B} \cdot \mathbf{x}' \mod q$ with overwhelming probability.

Efficiency. It is not hard to check that the underlying interactive procedure in previous section has communication cost $\widetilde{O}(l \cdot n)$; therefore, the resulting signature has bit-size $\widetilde{O}(\kappa \cdot l \cdot n + n) = \widetilde{O}(n \cdot \log N)$.

Now, we analyze the security requirements: anonymity, traceability, and non-frameability.

Theorem 4 (Anonymity)**.** *Assume that* COM *is a statistical hiding commitment scheme. Then, our NDRS scheme provides statistical anonymity in the random oracle model.*

Proof. We consider a sequence of games. The challenger $\mathcal{C}$ runs experiment $\mathbf{Exp}^{\mathsf{anon}-0}_{NDRS,\mathcal{A}}(n)$ in the first game, while, in the last one, it runs $\mathbf{Exp}^{\mathsf{anon}-1}_{NDRS,\mathcal{A}}(n)$.

Game $\mathbf{G}_0^{(b)}$: Exactly, it is the real experiment $\mathbf{Exp}^{\mathsf{anon}-b}_{NDRS,\mathcal{A}}(n)$, where the adversary is given a challenge signature $\Sigma^* \leftarrow \mathsf{Sign}(\mathsf{pp}, \{pk_{i_0}, pk_{i_1}\}, sk_{i_b}, M^*)$. Namely, given (i_0, i_1, M^*), the challenger $\mathcal{C}$ chooses a random $b \leftarrow \{0,1\}$ and computes a legitimate signature Σ^* using the secret key $sk_{i_b} = \mathbf{x}_{i_b}$ of user i_b:

1. Run $\mathsf{TAcc}(\mathbf{A}, R)$ and obtain $\mathbf{u} \in \{0,1\}^{nk}$, where $R = \{pk_{i_0}, pk_{i_1}\}$.
2. Run $\mathsf{TWitness}(\mathbf{A}, R, \mathbf{d}_{i_b})$ and obtain a witness w_{i_b} to the fact that $\mathbf{d}_{i_b} = \mathbf{A} \cdot \mathbf{x}_{i_b} \mod q \in R$.
3. Sample a seed $s \leftarrow \{0,1\}^n$, generate matrix $\mathbf{B} = \mathsf{PRG}(s) \in \mathbb{Z}_q^{n \times m}$ and compute $\mathbf{b} = \mathbf{B} \cdot \mathbf{x}_{i_b} \bmod q$. Then, produce a NIZKAoK Π with public input $(\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b})$ and prover's witness $(\mathbf{d}_{i_b}, w_{i_b}, \mathbf{x}_{i_b})$, i.e.,

$$\Pi = \big(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}_i\}_{i=1}^{\kappa}\big),$$

   where

$$\mathrm{CH} = \mathcal{H}_{\mathsf{FS}}\big(M^*, \{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}, R\big) \in \{1,2,3\}^{\kappa}.$$

4. Output $\Sigma^* = (\mathbf{B}, \mathbf{b}, \Pi)$.

Game $\mathbf{G}_1$: Generally, this game is identical to $\mathrm{G}_0^{(b)}$, except that the challenge signature Σ^* is made independent of the coin b, while preserving the statistical closeness to $\mathbf{G}_0^{(b)}$. In more detail, the following modifications are introduced with respect to $\mathbf{G}_0^{(b)}$:

1. In Step 3, we change how the vector $\mathbf{b}$ is generated. Specifically, $\mathcal{C}$ samples $\mathbf{b} \leftarrow \mathbb{Z}_q^n$ uniformly at random, instead of computing $\mathbf{b} = \mathbf{B} \cdot \mathbf{x}_{i_b} \mod q$.
2. In addition, in Step 3, the proof Π contained in the challenge signature Σ^* is produced in the simulation manner by $\mathcal{C}$'s programming on the random oracle $\mathcal{H}_{\mathsf{FS}}(\cdot)$.
   (a) For each $j \in [\kappa]$, choose a 'fake challenge' $\overline{Ch}_j \leftarrow \{1,2,3\}$ and prepare the 'commitment' CMT_j according to $\overline{Ch}_j$. Then, randomly pick a 'real challenge' $Ch_j \leftarrow \{1,2,3\} \backslash \{\overline{Ch}_j\}$.
   (b) Program the random oracle and set

$$\mathrm{CH} = \{Ch_j\}_{j=1}^{\kappa} = \mathcal{H}_{\mathsf{FS}}\big(M^*, \{\mathrm{CMT}_j\}_{j=1}^{\kappa}, \mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}, R\big).$$

(c) Prepare the 'response' $\{\mathrm{RSP}_j\}_{j=1}^{\kappa}$ in accordance with the normal procedure.

(d) Output

$$\Sigma^* = (s, \mathbf{b}, \Pi) = \left(s, \mathbf{b}, \{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}_i\}_{i=1}^{\kappa}\right).$$

Observe that, for each $j \in [\kappa]$, Ch_j is uniformly distributed in $\{1,2,3\}$, satisfying the requirement on the output of the random oracle. Besides, CMT_j and RSP_j are prepared in the same way as in Lemma A2 for proving the zero-knowledge property, implying that the challenge signature is valid. Finally, notice that the vector $\mathbf{b}$ in this game or $\mathbf{G}_0^{(b)}$ follows a uniform distribution over $\mathbb{Z}_q^n$. As a result, $\mathbf{G}_0^{(b)}$ and $\mathbf{G}_1$ are statistically indistinguishable.

Now, we obtain a sequence of indistinguishable games $\mathbf{G}_0^{(0)}$, $\mathbf{G}_1$ and $\mathbf{G}_0^{(1)}$. Since $\mathbf{G}_1$ is independent of the random coin b, the advantage of $\mathcal{A}$ in $\mathbf{G}_1$ is 0. Then, we have the advantage of $\mathcal{A}$ in $\mathbf{G}_0^{(0)}$ and $\mathbf{G}_0^{(1)}$ is negligible. This completes the proof. □

Next, we prove the traceability and the non-frameability. Before doing so, we first recall two useful lemmas.

Lemma 1 (Reference [8]). *For any matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a uniform random $\mathbf{x} \in \{0,1\}^m$, the probability that there exists another $\mathbf{x}' \in \{0,1\}^m \backslash \{\mathbf{x}\}$ such that $\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{x}' \bmod q$ is at least $1 - 2^{n \cdot \log q - m}$.*

Lemma 2 (Reference [13]). *Let $\mathcal{SS}$ be a signature scheme with security parameter n. Let $\mathcal{A}$ be a PPT algorithm whose input consists only of public data and which can ask $q_{\mathsf{H}} > 0$ queries to the random oracle. Assume that $\mathcal{A}$ produces within time bound T a valid signature $\left(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}_i\}_{i=1}^{\kappa}\right)$ of message M with probability ϵ. Then, within time $32 \cdot T \cdot q_{\mathsf{H}}/\epsilon$ and with probability $\epsilon' > 1/2$, a replay of $\mathcal{A}$ outputs 3 valid signatures of M:*

$$\left(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}^{(1)}, \{\mathrm{RSP}_i^{(1)}\}_{i=1}^{\kappa}\right), \quad \left(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}^{(2)}, \{\mathrm{RSP}_i^{(2)}\}_{i=1}^{\kappa}\right),$$
$$\left(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}^{(3)}, \{\mathrm{RSP}_i^{(3)}\}_{i=1}^{\kappa}\right)$$

for the same $\{\mathrm{CMT}_i\}_{i=1}^{\kappa}$ such that $\mathrm{CH}^{(1)}, \mathrm{CH}^{(2)}, \mathrm{CH}^{(3)}$ are pairwise distinct.

Theorem 5 (Traceability and Non-frameability). *Our NDRS scheme provides traceability and non-frameability in the random oracle model if the $\mathsf{SIVP}_{\tilde{O}(n)}$ is hard.*

Proof. Assume that there exists a PPT $\mathcal{A}$ has nonnegligible advantage ϵ in the experiment $\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$ or $\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$, i.e., $\mathcal{A}$ is able to output a valid signature Σ^* on message M^* under some ring $R^* = (pk_{i_0}, \ldots, pk_{i_r}) = (\mathbf{d}_0, \ldots, \mathbf{d}_r)$ such that

- either $\mathsf{EvidenceCheck}(\mathsf{pp}, R^*, i_j, \xi_{i_j}, \Sigma^*)$ will output 'disavowal' for each $j \in \{0, \ldots, r\}$, where ξ_{i_j} is a piece of evidence generated by user i_j;
- or $\mathsf{EvidenceCheck}(\mathsf{pp}, R^*, i_{j^*}, \xi_{i_{j^*}}, \Sigma^*)$ will output 'confirmation' for some honest user i_{j^*}.

We construct an algorithm $\mathcal{B}$ that solves the $\mathsf{SIVP}_{\tilde{O}(n)}$ problem with nonnegligible probability. Let $\mathsf{pp} = \mathbf{A}$. During the game, $\mathcal{B}$ generates the secrets of all the queried users as in the real scheme. With these secret keys, $\mathcal{B}$ is capable of faithfully answering all the queries. For the random oracle $\mathcal{H}_{\mathsf{FS}}(\cdot)$, we assume without loss of generality that: (1) $\mathcal{A}$ makes any given query to $\mathcal{H}_{\mathsf{FS}}(\cdot)$ only once; (2) if $\mathcal{A}$ outputs a signature, then $\mathcal{A}$ had previously queried $\mathcal{H}_{\mathsf{FS}}(\cdot)$.

When $\mathcal{A}$ halts, it outputs a valid triple (R^*, M^*, Σ^*), where

$$\Sigma^* = \left(s^*, \mathbf{b}^*, \{\mathrm{CMT^*}_i\}_{i=1}^{\kappa}, \mathrm{CH}^*, \{\mathrm{RSP^*}_i\}_{i=1}^{\kappa}\right).$$

We denote by $q_{\mathcal{H}}$ the upper bound on the number of queries that $\mathcal{A}$ makes to $\mathcal{H}_{\mathsf{FS}}(\cdot)$.

Then, by Lemma 2, when $\mathcal{B}$ runs up to $32 \cdot q_{\mathcal{H}}/\epsilon$ extra executions of $\mathcal{A}$ with the same random tap and inputs as in the first execution, with probability at least $1/2$, $\mathcal{A}$ will get a 3-fork responses $\mathrm{CH}^{(1)}, \mathrm{CH}^{(2)}, \mathrm{CH}^{(3)}$ (pairwise distinct) from the oracle $\mathcal{H}_{\mathsf{FS}}(\cdot)$.

With probability $1-(7/9)^{\kappa}$, there exists some $j \in [\kappa]$ for which the j-th bits of $\mathrm{CH}^{(1)}, \mathrm{CH}^{(2)}$, and $\mathrm{CH}^{(3)}$ are $\{Ch_j^{(1)}, Ch_j^{(2)}, Ch_j^{(3)}\} = \{1,2,3\}$. By the soundness of the argument system for the relation $\mathrm{R}_{\mathrm{NDRS}}$, $\mathcal{B}$ is able to extract a tuple $(\mathbf{d}^*, w^*, \mathbf{x}^*)$ from the responses $\mathrm{RSP}_j^{(1)}, \mathrm{RSP}_j^{(2)}, \mathrm{RSP}_j^{(3)}$ such that

$$\mathbf{A} \cdot \mathbf{x}^* = \mathbf{G} \cdot \mathbf{d}^* \mod q, \quad \mathsf{TVerify}(\mathbf{A}, \mathbf{u}^*, \mathbf{d}^*, w^*) = 1.$$

According to the value of $\mathbf{d}^*$, there are two cases:

- $\mathbf{d}^* \notin R^* = (\mathbf{d}_0, \ldots, \mathbf{d}_r)$. This means $\mathcal{B}$ can use $(R^*, \mathbf{d}^*, w^*)$ to break the security of the underlying accumulator, whose security is based on the assumption that $\mathsf{SIVP}_{\widetilde{O}(n)}$ is hard [8].
- $\mathbf{d}^* \in R^* = (\mathbf{d}_0, \ldots, \mathbf{d}_r)$, i.e., $\mathbf{d}^* = \mathbf{d}_{j^*}$. Note that the secret key $sk_{i_{j^*}}$ consists of a vector $\mathbf{x}_{i_{j^*}} \in \{0,1\}^m$ such that $\mathbf{A} \cdot \mathbf{x}_{i_{j^*}} = \mathbf{G} \cdot \mathbf{d}_{j^*} \mod q$. If $\mathbf{x}_{i_{j^*}} \neq \mathbf{x}^*$, then $\mathbf{x}_{i_{j^*}} - \mathbf{x}^* \in \{-1,0,1\}^m$ is a valid solution for the $\mathsf{SIS}_{n,m,q,1}$ instance $\mathbf{A}$.
  According to the experiments with respect to traceability and non-frameability, we distinguish the following two cases to discuss the probability that $\mathbf{x}_{i_{j^*}} \neq \mathbf{x}^*$.
  - In the experiment $\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$, $\mathcal{A}$ has corrupted user i_{j^*}, acts as the real malicious signer, and manages to evade the traceability. We claim that $\mathbf{x}_{i_{j^*}} \neq \mathbf{x}^*$, since $\mathcal{A}$ will otherwise be detected as the real singer by the algorithm $\mathsf{EvidenceCheck}(\mathsf{pp}, R^*, i_{j^*}, \xi_{i_{j^*}}, \Sigma)$, where $\xi_{i_{j^*}}$ contains an element $\mathbf{b} = \mathbf{B}^* \cdot \mathbf{x}_{i_{j^*}} \mod q$.
  - In the experiment $\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$, $\mathcal{A}$ did not corrupt user i_{j^*}, and temps to produce a valid signature such that the target victim i_{j^*} will be detected as the real signer. We claim that $\mathbf{x}_{i_{j^*}} \neq \mathbf{x}^*$ with probability greater than $1/2$ by the following two facts: (1) There exists another vector $\mathbf{x}^* \in \{0,1\}^m$ such that $\mathbf{A} \cdot \mathbf{x}^* = \mathbf{A} \cdot \mathbf{x}_{i_{j^*}} \mod q$ by Lemma 1. (2) The underlying argument system is zero-knowledge, which implies witness indistinguishability; thus, $\mathcal{A}$ can hardly get useful information from the signing queries.

In conclusion, in the experiment $\mathbf{Exp}^{\mathsf{trace}}_{NDRS,\mathcal{A}}(n)$ or $\mathbf{Exp}^{\mathsf{nf}}_{NDRS,\mathcal{A}}(n)$, a successful attacker $\mathcal{A}$ implies an attacker $\mathcal{B}$ that either defeats the soundness of the argument system, or breaks the security of the accumulator, or directly solves an $\mathsf{SIS}^{\infty}_{n,m,q,1}$ instance $\mathbf{A}$. Thus, our scheme provides traceability and non-frameability in the random oracle model, assuming that the $\mathsf{SIVP}_{\widetilde{O}(n)}$ problem is hard. □

5. Conclusions

In this work, we propose an efficient lattice-based NDRS scheme by using the techniques developed in Reference [8]. Our scheme has signature size only logarithmic to the ring size, and we prove its security in the random oracle model under the SIS assumption. Notice that, in our NDRS scheme, each secret key can only be used, at most, $k-1$ times for producing ring signatures, where $k = \log q$; otherwise, the secret key will be figured out from $\mathbf{B}$'s and corresponding $\mathbf{b}$'s. The direct way to increase the number of ring signatures for each user is to increase the parameter q, which will reduce efficiency. A better way is to develop new techniques that is able to authenticate the user's identity while producing the ring signature for relative small q. We leave it as a future work.

Author Contributions: Conceptualization, H.J. and Y.Z.; methodology, H.J. and Y.Z.; validation, C.T. and Y.Z.; investigation, H.J.; resources, Y.Z.; writing—original draft preparation, H.J.; writing—review and editing, C.T. and Y.Z.; funding acquisition, H.J. and C.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China grant number 2017YFB0802000, the Young Scientists Fund grant numbers 61802075, 61802241, 61902303, the National Natural Science Foundation of China grant numbers 61972457, U19B2021, the Guangdong Province Natural Science Foundation of Major Basic Research and Cultivation Project grant number 2015A030308016, the Project of Ordinary University Innovation Team Construction of Guangdong Province grant number 2015KCXTD014, the Collaborative Innovation Major Projects of Bureau of Education of Guangzhou City grant number 1201610005, the National Natural Science Foundation of Shaanxi Province grant number 2020ZDLGY08-04, Natural Science Basic Research Program of Shaanxi Province grant number 2020JQ-832.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Theorem 2

Our proof follows closely from that of Lemma 4 in Reference [8].

Completeness and Efficiency. It can be checked that the protocol has perfect completeness: if $\mathcal{P}$ is honest and follows the protocol, then $\mathcal{V}$ always outputs 1. The communication cost of the protocol is of order $\widetilde{O}(l \cdot m \cdot \log q) = \widetilde{O}(l \cdot n)$.

Lemma A1 (Zero-Knowledge Property)**.** *Assume that* COM *is a statistical hiding commitment scheme, then the protocol is a statistical zero-knowledge proof.*

Proof. To show the zero-knowledge property, we construct an efficient simulator $\mathcal{S}$ that outputs a simulated transcript statistically indistinguishable from the one produced by the honest prover.

The simulator $\mathcal{S}$ first randomly samples $\overline{Ch} \leftarrow \{1,2,3\}$, which serves as a prediction of the challenge value that $\hat{\mathcal{V}}$ will not choose.

$\overline{Ch} = 1$ First, $\mathcal{S}$ computes $\mathbf{x}' \in \mathbb{Z}_q^{2m}$, $\mathbf{v}'_1, \ldots, \mathbf{v}'_l \in \mathbb{Z}_q^m$ and $\mathbf{z}'_1, \ldots, \mathbf{z}'_l$, $\mathbf{y}'_1, \ldots, \mathbf{y}'_l \in \mathbb{Z}_q^{2m}$ such that

$$\begin{aligned}
\hat{\mathbf{A}} \cdot \mathbf{x}' &= \mathbf{G}^* \cdot \mathbf{v}'_l \mod q;\\
\hat{\mathbf{B}} \cdot \mathbf{x}' &= \mathbf{b} \mod q;\\
\mathbf{A}^* \cdot \mathbf{z}'_1 + \mathbf{A}^* \cdot \mathbf{y}'_1 &= \mathbf{G} \cdot \mathbf{u} \mod q;\\
\mathbf{A}^* \cdot \mathbf{z}'_{i+1} + \mathbf{A}^* \cdot \mathbf{y}'_{i+1} &= \mathbf{G}^* \cdot \mathbf{v}'_i \mod q \ \ \forall\, i \in [l-1].
\end{aligned}$$

Then, sample randomness ρ_1, ρ_2, ρ_3 for COM and

$$\begin{aligned}
&\tau \leftarrow \mathcal{S}_{2m};\ b_1, \ldots, b_l \leftarrow \{0,1\};\ \pi_1, \ldots, \pi_l,\ \phi_1, \ldots, \phi_l \leftarrow \mathcal{S}_m\\
&\mathbf{r}_{\mathbf{x}};\ \mathbf{r}_{\mathbf{v}_1}, \ldots, \mathbf{r}_{\mathbf{v}_l} \leftarrow \mathbb{Z}_q^m;\ \mathbf{r}_{\mathbf{z}_1}, \ldots, \mathbf{r}_{\mathbf{z}_l},\ \mathbf{r}_{\mathbf{y}_1}, \ldots, \mathbf{r}_{\mathbf{y}_l} \leftarrow \mathbb{Z}_q^{2m}.
\end{aligned}$$

Finally, send to $\mathcal{V}$ the commitment CMT=(C'_1, C'_2, C'_3), where

$$\begin{aligned}
C'_1 = \mathsf{COM}\big(&\tau;\ \hat{\mathbf{A}} \cdot \mathbf{r}_{\mathbf{x}} - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_l};\ \hat{\mathbf{B}} \cdot \mathbf{r}_{\mathbf{x}};\ \{b_i, \pi_i, \phi_i\}_{i=1}^{l};\ \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_1} + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_1};\\
&\{\mathbf{A}^* \cdot \mathbf{r}_{\mathbf{z}_{i+1}} + \mathbf{A}^* \cdot \mathbf{r}_{\mathbf{y}_{i+1}} - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}_i}\}_{i=1}^{l-1};\ \rho_1\big)\\
C'_2 = \mathsf{COM}\big(&\tau(\mathbf{r}_{\mathbf{x}});\ \{\pi_i(\mathbf{r}_{\mathbf{v}_i}), F_{b_i,\pi_i}(\mathbf{r}_{\mathbf{z}_i}), F_{\bar{b}_i,\phi_i}(\mathbf{r}_{\mathbf{y}_i})\}_{i=1}^{l};\ \rho_2\big)\\
C'_3 = \mathsf{COM}\big(&\tau(\mathbf{x}' + \mathbf{r}_{\mathbf{x}});\ \{\pi_i(\mathbf{v}'_i + \mathbf{r}_{\mathbf{v}_i}), F_{b_i,\pi_i}(\mathbf{z}'_i + \mathbf{r}_{\mathbf{z}_i}), F_{\bar{b}_i,\phi_i}(\mathbf{y}'_i + \mathbf{r}_{\mathbf{y}_i})\}_{i=1}^{l};\ \rho_3\big).
\end{aligned}$$

After receiving Ch from $\hat{\mathcal{V}}$, $\hat{\mathcal{S}}$ responds as follows:

- If $Ch = 1$: Output $\perp$ and abort.
- If $Ch = 2$: Send

$$\mathrm{RSP} = \big(\tau;\ \mathbf{x}' + \mathbf{r}_{\mathbf{x}};\ \{b_i, \pi_i, \phi_i, \mathbf{v}'_i + \mathbf{r}_{\mathbf{v}_i}, \mathbf{z}'_i + \mathbf{r}_{\mathbf{z}_i}, \mathbf{y}'\mathbf{r}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_1;\ \rho_3\big).$$

- If $Ch = 3$: Send

$$\mathrm{RSP} = \big(\tau;\ \mathbf{r}_{\mathbf{x}};\ \{b_i, \pi_i,\ \phi_i, \mathbf{r}_{\mathbf{v}_i}, \mathbf{r}_{\mathbf{z}_i}, \mathbf{r}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_1;\ \rho_2\big).$$

$\overline{Ch} = 2$ First, $\mathcal{S}$ samples

$$\begin{aligned}&\mathbf{x}' \leftarrow \mathsf{B}_{2m}^{m};\ j'_1, \ldots, j'_l \leftarrow \{0,1\};\ \mathbf{v}'_1, \ldots, \mathbf{v}'_l;\ \mathbf{w}'_1, \ldots, \mathbf{w}'_l \leftarrow \mathsf{B}_m^{nk};\\ &\tau \leftarrow \mathcal{S}_{2m};\ b_1, \ldots, b_l \leftarrow \{0,1\};\ \pi_1, \ldots, \pi_l,\ \phi_1, \ldots, \phi_l \leftarrow \mathcal{S}_m\\ &\mathbf{r}_{\mathbf{x}};\ \mathbf{r}_{\mathbf{v}_1}, \ldots, \mathbf{r}_{\mathbf{v}_l} \leftarrow \mathbb{Z}_q^m;\ \mathbf{r}_{\mathbf{z}_1}, \ldots, \mathbf{r}_{\mathbf{z}_l},\ \mathbf{r}_{\mathbf{y}_1}, \ldots, \mathbf{r}_{\mathbf{y}_l} \leftarrow \mathbb{Z}_q^{2m}.\end{aligned}$$

Then, compute $\mathbf{z}'_i = \mathsf{ext}(j'_i, \mathbf{v}'_i)$, $\mathbf{y}'_i = \mathsf{ext}(\bar{j}'_i, \mathbf{w}'_i)$ for each $j \in [l]$. Finally, send the commitment CMT computed as in case $\overline{Ch} = 1$.

After receiving Ch from $\hat{\mathcal{V}}$, $\hat{\mathcal{S}}$ responds as follows.

- If $Ch = 1$: Send

$$\mathrm{RSP} = \big(\tau(\mathbf{x}');\ \tau(\mathbf{r}_{\mathbf{x}});\ \{j'_i \oplus b_i, \pi_i(\mathbf{v}'_i), \phi_i(\mathbf{w}'_i), \pi_i(\mathbf{r}_{\mathbf{v}_i}), F_{b_i,\pi_i}(r_{\mathbf{z}_i}), F_{\bar{b}_i,\phi_i}(\mathbf{r}_{\mathbf{y}_i})\}_{i=1}^{l};\ \rho_1;\ \rho_3\big).$$

- If $Ch = 2$: Output $\perp$ and abort.
- If $Ch = 3$: Send RSP computed in the same manner as in the case $(\overline{Ch} = 1, Ch = 3)$.

$\overline{Ch} = 3$: First, $\mathcal{S}$ sample randomness as in the case $\overline{Ch} = 2$. Then, send the commitments CMT=(C'_1, C'_2, C'_3), where C'_2, C'_3 are computed as in $\overline{Ch} = 1$, and C'_1 is computed as

$$\begin{aligned}C'_1 = \mathsf{COM}\big(\tau;\ \hat{\mathbf{A}} \cdot (\mathbf{x}' + \mathbf{r}_{\mathbf{x}}) - \mathbf{G}^* \cdot (\mathbf{v}'_l + \mathbf{r}_{\mathbf{v}_l});\ \hat{\mathbf{B}} \cdot (\mathbf{x}' + \mathbf{r}_{\mathbf{x}});\ \{b_i, \pi_i, \phi_i\}_{i=1}^{l};\\ \mathbf{A}^* \cdot (\mathbf{z}'_1 + \mathbf{r}_{\mathbf{z}_1}) + \mathbf{A}^* \cdot (\mathbf{y}'_1 + \mathbf{r}_{\mathbf{y}_1}) - \mathbf{G} \cdot \mathbf{u};\\ \{\mathbf{A}^* \cdot (\mathbf{z}'_{i+1} + \mathbf{r}_{\mathbf{z}_{i+1}}) + \mathbf{A}^* \cdot (\mathbf{y}'_{i+1} + \mathbf{r}_{\mathbf{y}_{i+1}}) - \mathbf{G}^* \cdot (\mathbf{v}'_i + \mathbf{r}_{\mathbf{v}_i})\}_{i=1}^{l-1};\ \rho_1\big).\end{aligned}$$

After receiving Ch from $\hat{\mathcal{V}}$, $\hat{\mathcal{S}}$ responds as follows.

- If $Ch = 1$: Send RSP computed as in the case $(\overline{Ch} = 2, Ch = 1)$.
- If $Ch = 2$: Send RSP computed as in the case $(\overline{Ch} = 1, Ch = 2)$.
- If $Ch = 3$: Output $\perp$ and abort.

Because COM is statistically hiding, we have that, whenever $\mathcal{S}$ does not halt, it will output an accepting transcript, whose distribution is statistically close to that of the real prover. Besides, $\mathcal{S}$ halts with probability $1/3$. Therefore, $\mathcal{S}$ can successfully emulate the honest prover with probability $2/3$. □

To show the argument of knowledge property, it is enough to show that the protocol has the special soundness property [24].

Lemma A2 (Argument of Knowledge Property)**.** *Assume that* COM *is a statistical hiding commitment scheme, and then there exists an efficient knowledge extractor* $\mathcal{K}$ *that, given* 3 *valid responses* $(\mathrm{RSP}_1, \mathrm{RSP}_2, \mathrm{RSP}_3)$ *to the same commitment* CMT*, outputs a triple* $(\mathbf{d}', w', \mathbf{x}')$ *such that* $\big((\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{b}); \mathbf{d}', w', \mathbf{x}'\big) \in \mathrm{R}_{\mathrm{NDRS}}$.

Proof. Denote the 3 valid responses $(\mathrm{RSP}_1, \mathrm{RSP}_2, \mathrm{RSP}_3)$ to the same commitment CMT as follows:

$$\begin{aligned}
\mathrm{RSP}_1 &= \big(\widetilde{\mathbf{x}}^*;\ \widetilde{\mathbf{r}}_{\mathbf{x}};\ \{\widetilde{b}_i, \widetilde{\mathbf{v}}_i^*, \widetilde{\mathbf{w}}_i^*, \widetilde{\mathbf{r}}_{\mathbf{v}_i}, \widetilde{\mathbf{r}}_{\mathbf{z}_i}, \widetilde{\mathbf{r}}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_2;\ \rho_3\big),\\
\mathrm{RSP}_2 &= \big(\tau';\ \mathbf{s}_{\mathbf{x}};\ \{b_i', \pi_i', \phi_i', \mathbf{s}_{\mathbf{v}_i}, \mathbf{s}_{\mathbf{z}_i}, \mathbf{s}_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_1;\ \rho_3\big),\\
\mathrm{RSP}_3 &= \big(\tau'';\ \mathbf{r}'_{\mathbf{x}};\ \{b_i'', \pi_i'',\ \phi_i'', \mathbf{r}'_{\mathbf{v}_i}, \mathbf{r}'_{\mathbf{z}_i}, \mathbf{r}'_{\mathbf{y}_i}\}_{i=1}^{l};\ \rho_1;\ \rho_2\big).
\end{aligned}$$

The validity of RSP_1 implies that $\widetilde{\mathbf{x}}^* \in \mathsf{B}_{2m}^m$ and $\forall\, i \in [l]:\ \widetilde{\mathbf{v}}_i^*,\ \widetilde{\mathbf{w}}_i^* \in \mathsf{B}_m^{nk}$. Besides, we have:

$$\begin{aligned}
&\tau' = \tau'';\ \tau''(\mathbf{r}'_{\mathbf{x}}) = \widetilde{\mathbf{r}}_{\mathbf{x}};\ \tau'(\mathbf{s}_{\mathbf{x}}) = \widetilde{\mathbf{x}}^* + \widetilde{\mathbf{r}}_{\mathbf{x}},\\
&\hat{\mathbf{A}} \cdot \mathbf{s}_{\mathbf{x}} - \mathbf{G}^* \cdot \mathbf{s}_{\mathbf{v}_l} = \hat{\mathbf{A}} \cdot \mathbf{r}'_{\mathbf{x}} - \mathbf{G}^* \cdot \mathbf{r}_{\mathbf{v}'_l} \mod q,\\
&\hat{\mathbf{B}} \cdot \mathbf{s}_{\mathbf{x}} = \mathbf{b} + \hat{\mathbf{B}} \cdot \mathbf{r}'_{\mathbf{x}} \mod q,\\
&\mathbf{A}^* \cdot \mathbf{s}_{\mathbf{z}_1} + \mathbf{A}^* \cdot \mathbf{s}_{\mathbf{y}_1} - \mathbf{G} \cdot \mathbf{u} = \mathbf{A}^* \cdot \mathbf{r}'_{\mathbf{z}_1} + \mathbf{A}^* \cdot \mathbf{r}'_{\mathbf{y}_1} \mod q,
\end{aligned}$$

and, for each $i \in [l-1]$:

$$\mathbf{A}^* \cdot \mathbf{s}_{\mathbf{z}_{i+1}} + \mathbf{A}^* \cdot \mathbf{s}_{\mathbf{y}_{i+1}} - \mathbf{G}^* \cdot \mathbf{s}_{\mathbf{v}_i} = \mathbf{A}^* \cdot \mathbf{r}'_{\mathbf{z}_{i+1}} + \mathbf{A}^* \cdot \mathbf{r}'_{\mathbf{y}_{i+1}} - \mathbf{G}^* \cdot \mathbf{r}'_{\mathbf{v}_i} \mod q,$$

and, for all $i \in [l]$:

$$\begin{aligned}
&b_i' = b_i'';\ \pi' = \pi'';\ \phi' = \phi'',\\
&\pi_i'(\mathbf{s}_{\mathbf{x}}) = \widetilde{\mathbf{x}}^* + \widetilde{\mathbf{r}}_{\mathbf{x}};\ \pi_i''(\mathbf{r}'_{\mathbf{v}}) = \widetilde{\mathbf{r}}_{\mathbf{v}_i},\\
&F_{b_i', \pi_i'}(\mathbf{s}_{\mathbf{z}_i}) = \mathsf{ext}(\widetilde{b}_i, \widetilde{\mathbf{v}}_i^*) + \widetilde{\mathbf{r}}_{\mathbf{z}_i};\ F_{b_i'', \pi_i''}(\mathbf{r}'_{\mathbf{z}_i}) = \widetilde{\mathbf{r}}_{\mathbf{z}_i},\\
&F_{\bar{b}_i', \phi_i'}(\mathbf{s}_{\mathbf{y}_i}) = \mathsf{ext}(\bar{\widetilde{b}}_i, \widetilde{\mathbf{w}}_i^*) + \widetilde{\mathbf{r}}_{\mathbf{y}_i};\ F_{\bar{b}_i'', \phi_i''}(\mathbf{r}'_{\mathbf{y}_i}) = \widetilde{\mathbf{r}}_{\mathbf{y}_i}.
\end{aligned}$$

Now, the knowledge extractor $\mathcal{K}$ takes the following steps to extract the secret.

First, let $\mathbf{x}^* = \tau'^{-1}(\widetilde{\mathbf{x}}^*)$, and, for each $i \in [l]$, let

$$j_i = \widetilde{b}_i \oplus b_i';\ \mathbf{v}_i^* = \pi_i'^{-1}(\widetilde{\mathbf{v}}_i^*);\ \mathbf{w}_i^* = \phi_i'^{-1}(\widetilde{\mathbf{w}}_i^*);\ \mathbf{z}_i = \mathbf{s}_{\mathbf{z}_i} - \mathbf{r}'_{\mathbf{z}_i};\ \mathbf{y}_i = \mathbf{s}_{\mathbf{y}_i} - \mathbf{r}'_{\mathbf{y}_i}.$$

Note that $\mathbf{x}^* \in \mathsf{B}_{2m}^m$, and, for each $i \in [l]$, $\mathbf{v}_i^*,\ \mathbf{w}_i^* \in \mathsf{B}_m^{nk}$. Besides,

- $F_{b_i', \pi_i'}(\mathbf{z}_i) = \mathsf{ext}(\widetilde{b}_i, \widetilde{\mathbf{v}}_i^*) = \mathsf{ext}\big(j_i \oplus b_i', \pi'(\mathbf{v}_i^*)\big) \Leftrightarrow \mathbf{z}_i = \mathsf{ext}(j_i, \mathbf{v}_i^*)$,
- $F_{\bar{b}_i', \phi_i'}(\mathbf{y}_i) = \mathsf{ext}(\bar{\widetilde{b}}_i, \widetilde{\mathbf{w}}_i^*) = \mathsf{ext}\big(\bar{j}_i \oplus b_i', \phi'(\mathbf{w}_i^*)\big) \Leftrightarrow \mathbf{y}_i = \mathsf{ext}(\bar{j}_i, \mathbf{w}_i^*)$.

Further more, $\hat{\mathbf{A}} \cdot \mathbf{x}^* = \mathbf{G}^* \cdot \mathbf{v}_l^* \mod q$, $\hat{\mathbf{B}} \cdot \mathbf{x}^* = \mathbf{b} \mod q$ and

$$\begin{aligned}
\mathbf{A}^* \cdot \mathbf{z}_1 + \mathbf{A}^* \cdot \mathbf{y}_1 &= \mathbf{G} \cdot \mathbf{u} \mod q,\\
\mathbf{A}^* \cdot \mathbf{z}_{i+1} + \mathbf{A}^* \cdot \mathbf{y}_{i+1} &= \mathbf{G}^* \cdot \mathbf{v}_i^* \mod q\ \ \forall\, i \in [l-1],
\end{aligned}$$

which are equivalent to

$$\begin{aligned}
\mathbf{A}^* \cdot \mathsf{ext}(j_1, \mathbf{v}_1^*) + \mathbf{A}^* \cdot \mathsf{ext}(\bar{j}_1, \mathbf{w}_1^*) &= \mathbf{G} \cdot \mathbf{u} \mod q,\\
\mathbf{A}^* \cdot \mathsf{ext}(j_{i+1}, \mathbf{v}_{i+1}^*) + \mathbf{A}^* \cdot \mathsf{ext}(\bar{j}_{i+1}, \mathbf{w}_{i+1}^*) &= \mathbf{G}^* \cdot \mathbf{v}_i^* \mod q\ \ \forall\, i \in [l-1].
\end{aligned}$$

Then, $\mathcal{K}$ drops the last m coordinates from $\mathbf{x}^*$ and obtains $\mathbf{x}' \in \{0,1\}^m$. In addition, by dropping the last nk coordinates of $\mathbf{v}_1^*, \ldots, \mathbf{v}_l^*,\ \mathbf{w}_1^*, \ldots, \mathbf{w}_l^*$, it obtains $\mathbf{v}_1', \ldots, \mathbf{v}_l',\ \mathbf{w}_1', \ldots, \mathbf{w}_l' \in \{0,1\}^{nk}$. Observe that $\mathbf{A} \cdot \mathbf{x}' = \mathbf{G} \cdot \mathbf{v}_l' \mod q$, $\mathbf{B} \cdot \mathbf{x}' = \mathbf{b} \mod q$. Thus, the following relations holds:

$$\begin{aligned}
\mathbf{A} \cdot \mathsf{ext}(j_1, \mathbf{v}_1') + \mathbf{A} \cdot \mathsf{ext}(\bar{j}_1, \mathbf{w}_1') &= \mathbf{G} \cdot \mathbf{u} \mod q,\\
\mathbf{A} \cdot \mathsf{ext}(j_{i+1}, \mathbf{v}_{i+1}') + \mathbf{A} \cdot \mathsf{ext}(\bar{j}_{i+1}, \mathbf{w}_{i+1}') &= \mathbf{G} \cdot \mathbf{v}_i' \mod q\ \ \forall\, i \in [l-1],
\end{aligned}$$

which are equivalent to

$$\begin{aligned}\mathbf{v}'_0 &= \mathbf{u},\\ \mathbf{v}'_i &= \bar{j}_{i+1} \cdot h_{\mathbf{A}}(\mathbf{v}'_{i+1}, \mathbf{w}'_{i+1}) + j_{i+1} \cdot h_{\mathbf{A}}(\mathbf{w}'_{i+1}, \mathbf{v}'_{i+1}).\end{aligned}$$

Finally, let $\mathbf{d}' = \mathbf{v}'_l$ and $w' = \big((j_1, \ldots, j_l), (\mathbf{w}'_l, \ldots, \mathbf{w}'_1)\big)$, then $\mathsf{Verify}(\mathbf{A}, \mathbf{u}, \mathbf{d}', w') = 1$, and output $\mathbf{d}', w', \mathbf{x}'$, which satisfy

$$\big((\mathbf{A}, \mathbf{B}, \mathbf{u}, \mathbf{d}), \mathbf{d}', w', \mathbf{x}'\big) \in \mathrm{R}_{\mathrm{NDRS}}.$$

This concludes the proof. □

References

1. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret: Theory and applications of ring signatures. *Theor. Comput. Sci.* **2006**, *3895*, 164–186.
2. Naor, M. Deniable ring authentication. In *CRYPTO 2002, Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 481–498.
3. Dodis, Y.; Kiayias, A.; Nicolosi, A.; Shoup, V. Anonymous identification in *Ad Hoc Groups*. In *EUROCRYPT 2004, Proceedings of the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 609–626.
4. Chaum, D.; van Heyst, E. Group signatures. In *EUROCRYPT 1991, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, 8–11 April 1991*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 257–265.
5. Bellare, M.; Micciancio, D.; Warinschi, B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT 2003, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 4–8 May 2003*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 614–629.
6. Boyen, X.; Waters, B. Compact group signatures without random oracles. In *EUROCRYPT 2006, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, 28 May–1 June 2006*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 427–444.
7. Groth, J. Fully anonymous group signatures without random oracles. In *ASIACRYPT 2007, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 164–180.
8. 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 *EUROCRYPT 2016, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 8–12 May 2016*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–31.
9. Ling, S.; Nguyen, K.; Wang, H.; Xu, Y. Lattice-based group signatures: Achieving full dynamicity (and deniability) with ease. *Theor. Comput. Sci.* **2019**, *783*, 71–94. [CrossRef]
10. Komano, Y.; Ohta, K.; Shimbo, A.; Kawamura, S. Toward the fair anonymous signatures: Deniable ring signatures. In *CT-RSA 2006, Proceedings of the Cryptographers' Track at the RSA Conference, San Jose, CA, USA, 13–17 February 2006*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 174–191.
11. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput* **1997**, *26*, 1484–1509. [CrossRef]
12. Gao, W.; Chen, L.; Hu, Y.; Newton, C.J.; Wang, B.; Chen, J. Lattice-based deniable ring signatures. *Int. J. Inf. Secur.* **2019**, *18*, 355–370. [CrossRef]
13. Cheng, S.; Nguyen, K.; Wang, H. Policy-based signature scheme from lattices. *Des. Codes Cryptogr.* **2016**, *81*, 43–74. [CrossRef]
14. Libert, B.; Ling, S.; Nguyen, K.; Wang, H. Zero-knowledge arguments for lattice-based PRFs and applications to e-cash. In *ASIACRYPT 2017, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017*; Springer: Cham, Switzerland, 2017; pp. 304–335.
15. Stern, J. A new paradigm for public key identification. *IEEE Trans. Inf. Theory* **1996**, *42*, 1757–1768. [CrossRef]
16. Jia, H.; Tang, C. Cryptanalysis of a non-interactive deniable ring signature scheme. *Int. J. Inf. Secur.* **2020**, *20*, 103–112. [CrossRef]
17. Ajtai, M. Generating hard instances of lattice problems. *Quad. Mat.* **2004**, *13*, 1–32.
18. Micciancio, D.; Regev, O. Worst-case to average-case reductions based on Gaussian measure. *SIAM J. Comput.* **2007**, *37*, 267–302. [CrossRef]
19. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In *STOC 2008, Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 17–20 May 2008*; ACM: Denver, CO, USA, 2008; pp. 197–206.
20. Micciancio, D.; Peikert, C. Hardness of SIS and LWE with small parameters. In *CRYPTO 2013, Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 21–39.

21. Jain, A.; Krenn, S.; Pietrzak, K.; Tentes, A. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT 2012, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 2–6 December 2012*; Springer: Cham, Switzerland, 2012; pp. 663–680.
22. Benhamouda, F.; Camenisch, J.; Krenn, S.; Lyubashevsky, V.; Neven, G. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *ASIACRYPT 2014, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, 7–11 December 2014*; Springer: Cham, Switzerland, 2014; pp. 551–572.
23. Kawachi, A.; Tanaka, K.; Xagawa, K. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT 2008, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, VIC, Australia, 7–11 December 2008*; Springer: Cham, Switzerland, 2008; pp. 372–389.
24. Groth, J. Evaluating security of voting schemes in the universal composability framework. In *ACNS 2004, Proceedings of the InInternational Conference on Applied Cryptography and Network Security, Yellow Mountains, China, 8–11 June 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 46–60.