

# Efficient and Post-Quantum Zero-Knowledge Proofs for Blockchain Confidential Transaction Protocols

Shang GAO<sup>1</sup>, Tianyu ZHENG<sup>1</sup>, Yu GUO<sup>2</sup>, and Bin XIAO<sup>1</sup>

<sup>1</sup> The Hong Kong Polytechnic University, Hong Kong, China

<sup>2</sup> SECBIT Labs, Suzhou, China

{shanggao,tianzheng,csbxiao}@polyu.edu.hk

yu.guo@secbit.io

**Abstract.** We propose new zero-knowledge proofs for efficient and post-quantum ring confidential transaction (RingCT) protocols based on lattice assumptions in Blockchain systems. First, we introduce an inner-product based linear equation satisfiability approach for balance proofs with a wide range (e.g. 64-bit precision). Unlike existing balance proofs that require additional proofs for some “corrector values” [CCS’19], our approach avoids the corrector values for better efficiency. Furthermore, we design a ring signature scheme to efficiently hide a user’s identity in large anonymity sets. Different from existing approaches that adopt a one-out-of-many proof [CCS’19, Crypto’19], we show that a linear sum proof suffices in ring signatures which could avoid the costly binary proof part. We further use the idea of “unbalanced” relations to build a logarithmic-size ring signature scheme. Finally, we show how to adopt these techniques in RingCT protocols and implement a prototype to compare the performance with existing approaches. The results show our solutions can reduce about 25% proof size of Crypto’19, and up to 70% proof size, 30% proving time, and 20% verification time of CCS’19. We also believe our techniques are of independent interest for other privacy-preserving applications such as secure e-voting and are applicable in a generic setting.

**Keywords:** Lattice-based cryptography, zero-knowledge proof, balance proof, ring signature, RingCT, blockchain

## 1 Introduction

Cryptocurrencies adopt the blockchain technique where each participant maintains a ledger of all transactions to avoid any tampering attempts from minority attackers. In private/anonymous cryptocurrencies, the amount<sup>3</sup> stored in each

---

<sup>3</sup> In this paper, the “amount” refers to “account balance”. We avoid using balance here as it conflicts with the notion of “balance” in balance proofs.

account and the user’s identity need to be hidden from the outside world. Meanwhile, it also requires public verification to ensure each transaction is valid. Existing solutions such as Monero [32] and Zcash [34] adopt zero-knowledge proofs (ZKPs) to prove useful statements without leaking any private information. For instance, in Monero, a ring confidential transaction (RingCT) protocol is used with a *range proof* to show all amounts are non-negative and the difference between outputs and inputs is zero (balance property), and a *ring signature*-like approach to hide the identity of a spender with one-out-of-many proofs [28]. However, as the security of these implementations is mainly based on discrete logarithm assumptions, current anonymous cryptocurrencies are at risk of potential attacks from quantum computers.

This deficiency has impelled the development of “post-quantum” solutions. Among all approaches, lattice-based cryptography is one of the most promising candidates based on computational lattice problems. Unfortunately, the costs of lattice-based solutions increase significantly in comparison with those in discrete logarithm settings. Taking the range proof in Crypto’19 [14] as an example, a single proof costs nearly 200KB size while the Bulletproofs protocol [10] costs less than 1KB. Even worse, as the amounts in a RingCT protocol need to be committed separately, the efficient aggregation approach in [14] cannot be adopted. MatRiCT (CCS’19 [17]) is the state-of-the-art lattice-based RingCT protocol to optimize the proof size in a blockchain environment. By using a novel balance proof with hashed-message commitments (HMC) to show a transaction is valid, MatRiCT reduces the size of commitments and allows proofs on a wide range. Furthermore, it adopts techniques such as batched commitments and rejection sampling for secrets with a fixed Hamming weight in one-out-of-many proofs to improve the efficiency of the ring signature. However, the balance proof in MatRiCT requires some “corrector values” to show the amount difference is a commitment to zero. Proving the corrector values are properly generated imposes a prohibitive cost on balance proofs [17].

The main goal of this paper is to propose efficient, scalable, and post-quantum<sup>4</sup> ZKPs under for lattice-based RingCT protocols (e.g., MatRiCT). We first take an in-depth analysis of the balance proof and ring signature in MatRiCT and discover several interesting revelations (Section 3). Based on our analysis, we leverage an inner-product relation to prove the linear equation satisfiability for balance proofs and propose an “unbalanced” linear sum proof for ring signatures (Section 4). We further design a novel linear equation satisfiability proof and a new ring signature scheme which are more efficient than existing approaches (Section 5). With these techniques, we propose efficient post-quantum ZKPs for RingCT protocols (Section 6). We also implement a prototype and compare the performance with state-of-the-art solutions (Section 7). Finally, we discuss some extensions (Section 8) and general applications (Section 9) of our techniques.

---

<sup>4</sup> The post-quantum security referred in this paper relies on the hardness of “post-quantum” lattice assumptions and does not necessarily involve security proofs in quantum random oracle model [11, 22]. We only use ROM for Fiat-Shamir transformation in the security analysis, as with [12, 14–17].

We conclude our revelations as follows:

- *“Corrector values” are unnecessary in a balance proof.* We analyze the balance proof in MatRiCT and find the corrector values can be reduced without sacrificing the security of the proof (Section 3.1).
- *Inner-product relation is efficient in proving linear equation satisfiability.* Based on our observation, we generalize balance proofs to a linear equation satisfiability (Section 4.1 and 5.1) and show a more efficient balance proof for RingCT protocol (Section 6.1).
- *The binary proof is redundant in ring signatures.* We analyze existing ring signatures (one-out-of-many proofs) and show the binary proof used in these approaches requires a larger parameter set. Furthermore, we prove it is sufficient to use a linear sum proof for ring signatures without the binary proof part in a one-out-of-many proof (Section 3.2).
- *Unbalanced linear sum proof is secure and efficient for ring signatures.* To propose an efficient ring signature scheme, we leverage the idea of relaxed relation and build our linear sum proof with an “unbalanced” relation (Section 4.2 and 5.2). Furthermore, we design an efficient ring signature scheme based on the unbalanced linear sum proof (Section 6.2).

## 2 Preliminaries

### 2.1 Related Work

In anonymous cryptocurrencies, RingCT protocols [17, 28, 35, 38] adopt *range proofs* to show transaction amounts are valid and *ring signature*-like approaches to hide a spender’s identity. We describe existing work in these two directions.

**Range proofs.** To guarantee the amount of each account in a confidential transaction is valid, range proofs [10, 29, 31] are used in RingCT protocols. By encapsulating the amounts in homomorphic commitments, the prover proves that 1) all the inputs and outputs are non-negative and 2) the sum of inputs equals outputs. The proofs can be succinct and efficient with a trusted setup [5, 18, 20, 30], but will undermine the decentralized property of blockchain systems at the same time where no particular trusted authority should be involved. Though the trusted setup can be replaced by a secure multi-party computation, the process is costly and may not be reusable when the application (i.e., circuit) is updated [5, 20]. Currently, the smallest proof without a trusted setup is the Bulletproofs protocol [10], which leverages the vector compression idea in [7]. However, these approaches fail to address quantum attacks as they are proposed based on discrete logarithm assumptions.

One of the most promising post-quantum cryptography candidates is lattice-based cryptography. Esgin et al. propose new range proofs in lattice settings based on the unbounded-message commitment (UMC) scheme and further adopt a new packing technique for efficient batch processing [14]. Unfortunately, the size of a UMC commitment is linear to the message size which is not suitable for large values such as amounts of different accounts. Besides, the batch processing

in [14] is only efficient when the amounts of all accounts are committed together in a single commitment, while the amounts are usually committed separately in a RingCT protocol. The state-of-the-art lattice-based RingCT approach is MatRiCT [17]. Instead of using UMC to commit to an amount directly, MatRiCT commits to the bits of an amount with HMC [15] and further adopts a balance proof with some “corrector values” to show the sums of inputs and outputs are equal. Esgin et al. also show the proof size and running time can be reduced by optimizing the underlying cyclotomic rings [16]. Though the efficiency has improved comparing with [14], a subtle issue prevents the use of MatRiCT in general cases: the corrector values require additional range proofs when dealing with multiple input and output accounts (more details in Section 3.1).

**Ring signatures.** To hide the identity of a signer, ring signatures (one-out-of-many proofs) allow one to prove the knowledge of a secret key corresponding to an element in a set of public keys. The idea of the ring signature is proposed by Rivest, Shamir, and Tauman [33]. In discrete logarithm settings, logarithmic-size ring signatures [6, 21] have been used in different applications. Most of current anonymous cryptocurrencies are implemented based on discrete logarithm assumptions which cannot provide post-quantum security.

On the side of lattice settings, linear-size ring signatures have been proposed [4, 26, 36], but these approaches are inefficient for large anonymous groups. Libert et al. [25] design a Merkle tree based accumulator and build a ZKP system for this accumulator. With these tools, logarithmic-size ring and group signatures are proposed. Furthermore, a linkable version of [25] (signatures created by the same signer can be linked) is introduced in [37]. Though the signature size of [25, 37] is logarithmic, the zero-knowledge arguments applied in the accumulator require multiple protocol iterations (multi-shot proofs) to get a negligible soundness error. Esgin et al. [15] introduce new tools for ZKPs to extend the discrete logarithm proof techniques in [6, 21] to lattice settings. Logarithmic-size ring signatures can be easily achieved with these new techniques. A further improvement in [14] makes the underlying ZKPs achieve a negligible soundness error at a single protocol iteration (i.e., one-shot proof in Section 2.6) and reduces the signature size accordingly. Following the blueprint of [14], MatRiCT [17] batches commitments in binary proofs and improves the rejection sampling to build a more efficient ring signature scheme. Besides, MatRiCT uses two sets of compatible parameters for the ring signature to reduce the size (discussed in Section 3.2).

## 2.2 Notations

We use  $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$  to denote the ring of integers modulo  $q$  represented by the range  $[-\frac{q-1}{2}, \frac{q-1}{2}]$ . The rings are defined by  $R = \mathbb{Z}[X]/(X^d + 1)$  and  $R_q = \mathbb{Z}_q[X]/(X^d + 1)$  where  $d > 1$  is a power of 2. Bold-face lower-case letters such as  $\mathbf{a}$  and bold-face capital letters such as  $\mathbf{A}$  are used to denote column vectors and matrices respectively. Commitments are denoted by capital letters such as  $C$  even though they may be vectors. We use  $(\mathbf{a}, \mathbf{b})$  to denote appending vector  $\mathbf{a}$  to

**b.** For a vector  $\mathbf{a} = (a_0, \dots, a_{k-1})$ , the norms are defined as  $\|\mathbf{a}\| = \sqrt{\sum_{i=0}^{k-1} a_i^2}$ ,  $\|\mathbf{a}\|_1 = \sum_{i=0}^{k-1} |a_i|$ , and  $\|\mathbf{a}\|_\infty = \max_i |a_i|$ . The norms of a polynomial are defined in a similar way as a vector. Suppose  $x \in \mathbb{Z}_q$ , we denote  $\mathbf{x}^k = (1, x, x^2, \dots, x^{k-1})$ . Furthermore, the inner-product of two  $k$ -dimensional vectors  $\mathbf{a}$  and  $\mathbf{b}$  is denoted as  $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=0}^{k-1} a_i b_i$  and the Hadamard product is denoted as  $\mathbf{a} \circ \mathbf{b} = (a_0 \cdot b_0, \dots, a_{k-1} \cdot b_{k-1})$ . The Kronecker's delta is denoted as  $\delta_{j,i}$  such that  $\delta_{j,i} = 1$  when  $j = i$  and otherwise  $\delta_{j,i} = 0$ .  $HW(x)$  denotes the Hamming weight of the coefficient vector of  $x \in R$ . Uniform distribution on a set  $S$  is denoted by  $\mathcal{U}(S)$ , and  $a \leftarrow \mathcal{S}$  denotes sampling  $a$  from a distribution  $\mathcal{S}$ , or uniformly sampling from a set  $\mathcal{S}$ .  $\mathcal{S}^{md}$  indicates that totally  $md$  coefficients are sampled to generate  $m$  polynomials in  $R$  of degree  $d$ .  $\mathfrak{L}_{\mathcal{B}}$  denotes the set of polynomials in  $R$  with infinity norm at most  $\mathcal{B} \in \mathbb{Z}^*$ .

The challenge space in a  $\Sigma$ -protocol is defined as follows:

$$\mathcal{C} = \{x \in R : \deg(x) = d - 1 \wedge HW(x) = w \wedge \|x\|_\infty = p\}. \quad (1)$$

Clearly, we can observe  $\|x\|_1 \leq pw$  and  $|\mathcal{C}| = \binom{d}{w} \cdot (2p)^w$ . We denote all non-zero challenges as  $\mathcal{C}^*$ .

**Lemma 1. (Lemma 3 in [14])** For any  $y_1, \dots, y_n \in \mathcal{C}^*$ , we have  $\|\prod_{i=1}^n y_i\|_\infty \leq (2p)^n \cdot w^{n-1}$  and  $\|\prod_{i=1}^n y_i\| \leq \sqrt{d} \cdot (2p)^n \cdot w^{n-1}$ .

### 2.3 Rejection Sampling

In  $\Sigma$ -protocols, a prover needs to encode its witness  $\mathbf{b}$  as  $\mathbf{f}$  with a challenge  $x$  and a randomness  $\mathbf{a}$ ,  $\mathbf{f} = x\mathbf{b} + \mathbf{a}$ . In the M-SIS assumption (described in Section 2.4), it is important to hide the distribution of  $\mathbf{b}$  from the distribution of  $(x, \mathbf{f})$ . The most commonly used approach is the rejection sampling to restrict the distribution of  $(x, \mathbf{f})$  being independent of  $\mathbf{b}$  by rejecting  $\mathbf{f}$  which are out of bounds [27]. We summarize rejection sampling in Algorithm 1, where  $T = \|\mathbf{b}\|$  and  $\phi$  is a positive value to control the deviation of the normal distribution. Note that this algorithm returns 1 (not abort) so as to re-sample  $\mathbf{a}$  when  $\mathbf{f}$  is rejected by Algorithm 1.

---

#### Algorithm 1 Rejection Sampling

---

$\text{Rej}(\mathbf{f}, \mathbf{b}, \phi, T)$

- 1:  $\sigma = \phi T$ ;  $\mu(\phi) = \exp(\frac{12}{\phi} + \frac{1}{2\phi^2})$ ;  $u \leftarrow [0, 1)$
  - 2: **if**  $u > \frac{1}{\mu(\phi)} \cdot \exp(\frac{-2\langle \mathbf{f}, \mathbf{b} \rangle + \|\mathbf{b}\|^2}{2\sigma^2})$  **then**
  - 3:   Return  $\perp$
  - 4: **end if**
  - 5: Return 1
-

## 2.4 M-SIS and M-LWE Problems

We define the two well-known lattice problems [23], module short integer solution (M-SIS) and module learning with errors (M-LWE), which our schemes' security relies on.

**Definition 1.** *M-SIS*( $n, m, q, \gamma$ ). Given  $\mathbf{A} \leftarrow R_q^{n \times m}$ , the goal of the problem is to find  $\mathbf{z} \in R_q^m$  such that  $\mathbf{A}\mathbf{z} = \mathbf{0} \pmod{q}$  and  $0 < \|\mathbf{z}\| \leq \gamma$ .

**Definition 2.** *M-LWE*( $n, m, q, \mathcal{B}$ ). Given  $\mathfrak{U}_{\mathcal{B}}$  be a distribution over  $R_q$  and  $\mathbf{s} \leftarrow \mathfrak{U}_{\mathcal{B}}^n$  be a secret key. Define *LWE*( $q, \mathbf{s}$ ) as the distribution obtained by sampling  $\mathbf{a} \leftarrow R_q^n$ ,  $e \leftarrow \mathfrak{U}_{\mathcal{B}}$  and outputting  $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$ . The goal of the problem is to distinguish between  $m$  given samples from either *LWE*( $q, \mathbf{s}$ ) or  $\mathcal{U}(R_q^n, R_q)$ .

## 2.5 Hashed-Message Commitment

Let  $n, m, \mathcal{B}, q$  be positive integers with  $m > n$ . Suppose a prover commits to  $v$ -dimensional vectors over  $R_q$  for  $v \geq 1$ . The instantiation of the hashed-message commitment (HMC) scheme [3, 17] is as follows:

- **CKeygen**( $1^\lambda$ ): Sample  $\mathbf{G}_r \leftarrow R_q^{n \times m}$  and  $\mathbf{G}_m \leftarrow R_q^{n \times v}$ . Output  $ck = \mathbf{G} = (\mathbf{G}_r, \mathbf{G}_m) \in R_q^{n \times (m+v)}$ .
- **Commit** <sub>$ck$</sub> ( $\mathbf{m}$ ): Sample  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$ . Output  $\mathbf{r}$  and  $\text{Com}_{ck}(\mathbf{m}, \mathbf{r}) = \mathbf{G} \cdot (\mathbf{r}, \mathbf{m}) = \mathbf{G}_r \cdot \mathbf{r} + \mathbf{G}_m \cdot \mathbf{m}$ .
- **COpen** <sub>$ck$</sub> ( $C, (y, \mathbf{m}', \mathbf{r}')$ ): If  $\|(\mathbf{m}', \mathbf{r}')\| \leq \gamma$  and  $yC = \text{Com}_{ck}(\mathbf{m}', \mathbf{r}')$  return 1, otherwise return 0.

**Remarks.** As all operations are conducted on  $R_q$ , the prover needs to sample  $md$ -many  $\mathbb{Z}_q$  elements to build an  $m$ -dimensional  $R_q$  vector in **Commit**. Furthermore, the opening algorithm **COpen** does not simply check  $C \stackrel{?}{=} \text{Com}_{ck}(\mathbf{m}', \mathbf{r}')$  in common lattice-based schemes [12], but with a relaxation factor  $y \in R_q$  as in [8, 14, 17]. This is due to the straightforward soundness proofs under lattice assumptions do not work. Thus, we use “relaxed relations” by relaxing the verification relation to overcome the complications. Besides, the verifier also needs to check the norm of the openings,  $\|(\mathbf{m}', \mathbf{r}')\| \leq \gamma$ , to ensure the hardness of M-SIS problem in Definition 1.

**Lemma 2. (Lemma 2.3 in [17])** For a (large) set of appropriately chosen parameters, if *M-LWE*( $m - n, m, q, \mathcal{B}$ ) problem is hard then the HMC defined above is computationally hiding. If *M-SIS*( $n, m + v, q, 2\gamma_{com}$ ) is hard, then the HMC defined above is computationally strong  $\gamma_{com}$ -binding to the same relaxation factor  $y$ .

## 2.6 Vandermonde Matrix and One-Shot Proof [14]

A  $(k + 1)$ -dimensional Vandermonde matrix  $\mathbf{V}$  is defined as follows for some  $x_0, \dots, x_k \in \mathcal{R}$ :

$$\mathbf{V} = \begin{pmatrix} 1 & x_0 & \cdots & x_0^k \\ 1 & x_1 & \cdots & x_1^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^k \end{pmatrix}. \quad (2)$$

Let  $\text{adj}(\mathbf{V})$  denotes adjugate matrix of  $\mathbf{V}$  and  $\det(\mathbf{V})$  denotes the determinant of  $\mathbf{V}$ . Considering the property  $\text{adj}(\mathbf{V}) \cdot \mathbf{V} = \det(\mathbf{V}) \cdot \mathbf{I}_{k+1}$ , we have

$$\det(\mathbf{V}) = \prod_{0 \leq i < j \leq k} (x_j - x_i). \quad (3)$$

Let  $(\Gamma_0, \dots, \Gamma_k)$  be the last row of  $\text{adj}(\mathbf{V})$ . Then

$$\Gamma_i = (-1)^{i+k} \prod_{\substack{0 \leq s < j \leq k \\ s, j \neq i}} (x_j - x_s). \quad (4)$$

**Lemma 3.** (*Lemma 4 in [14]*) Let  $\kappa = \frac{k(k+1)}{2}$ , we have  $\|\det(\mathbf{V})\|_\infty \leq (2p)^\kappa w^{\kappa-1}$  when using the challenge space in Equation (1).

The one-shot proof is a technique proposed in [14] to efficiently prove non-linear polynomial relations. Consider a  $k$ -degree polynomial relation with commitments  $C_0 = \text{Com}(\mathbf{m}_0; \mathbf{r}_0), \dots, C_k = \text{Com}(\mathbf{m}_k; \mathbf{r}_k)$ . The prover encodes the message as  $(\mathbf{f}, \mathbf{z}) \leftarrow (\sum_{i=0}^k x^i \mathbf{m}_i, \sum_{i=0}^k x^i \mathbf{r}_i)$  with a challenge  $x$ . The verifier checks the norms of  $\mathbf{f}, \mathbf{z}$  and  $\sum_{i=0}^k x^i C_i \stackrel{?}{=} \text{Com}(\mathbf{f}; \mathbf{z})$ . This protocol has  $(k+1)$ -special soundness as we can extract a witness in one shot with the following approach.

Considering  $(k+1)$  accepted transactions with distinct challenges  $x_i$ 's and responses  $(\mathbf{f}_i, \mathbf{z}_i)$ 's where  $i \in [0, k]$  ( $C_i$ 's are the same). We have the following relation

$$\begin{pmatrix} 1 & x_0 & \cdots & x_0^k \\ 1 & x_1 & \cdots & x_1^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^k \end{pmatrix} \cdot \begin{pmatrix} C_0 \\ C_1 \\ \vdots \\ C_k \end{pmatrix} = \begin{pmatrix} \text{Com}(\mathbf{f}_0; \mathbf{z}_k) \\ \text{Com}(\mathbf{f}_1; \mathbf{z}_k) \\ \vdots \\ \text{Com}(\mathbf{f}_k; \mathbf{z}_k) \end{pmatrix}. \quad (5)$$

Let the Vandermonde matrix in Equation (5) be  $\mathbf{V}$ . By multiplying both sides of Equation (5) by  $\text{adj}(\mathbf{V})$ , based on Equation (4), its last row becomes

$$\begin{aligned} \det(\mathbf{V}) \cdot C_k &= \sum_{i=0}^k \Gamma_i \text{Com}(\mathbf{f}_i; \mathbf{z}_i) \\ &= \text{Com}\left(\sum_{i=0}^k \Gamma_i \mathbf{f}_i; \sum_{i=0}^k \Gamma_i \mathbf{z}_i\right) := \text{Com}(\widehat{\mathbf{m}}_k; \widehat{\mathbf{r}}_k). \end{aligned} \quad (6)$$

Therefore,  $(\widehat{\mathbf{m}}_k, \widehat{\mathbf{r}}_k)$  is an exact opening of  $yC_k$  with a relaxation factor  $y = \det(\mathbf{V})$ .

**Lemma 4.** (*Lemma 5 in [14]*) *In Equation (6), the following holds for  $\kappa' = \frac{k(k-1)}{2}$ :*

$$\begin{aligned} \|\widehat{\mathbf{m}}_k\| &\leq d(k+1)(2p)^{\kappa'} w^{\kappa'-1} \cdot \max_i \|\mathbf{f}_i\|, \\ \|\widehat{\mathbf{r}}_k\| &\leq d(k+1)(2p)^{\kappa'} w^{\kappa'-1} \cdot \max_i \|\mathbf{z}_i\|. \end{aligned} \tag{7}$$

### 3 Observations and Techniques

We first analyze the balance proof and ring signature scheme in MatRiCT [17]. Then we show the performance of these approaches can be further improved with our new techniques.

#### 3.1 Corrector Values in Balance Proofs

In existing RingCT protocols, to prove a transaction is valid, a spender (prover) needs to show 1) all the inputs and outputs are non-negative and 2) the difference between inputs and outputs is zero. The former relation can be checked in a range proof while the latter one is quite simple as  $\text{Com}(a_1; *) + \text{Com}(a_2; *) = \text{Com}(a_1 + a_2; *)$  holds under a homomorphic commitment scheme. In lattice settings, most approaches use UMC to commit to an unbounded secret like amount [3, 14]. However, as the size of a UMC commitment grows linearly with the secret size, using a range proof directly is not practical in lattice-based RingCT protocols.

MatRiCT [17] commits to bits of each amount with HMC to avoid the cost of UMC. Thus, the former relation can be proved in a binary proof. For the latter one, it requires “corrector values” to ensure  $\text{Bits}(a_1) + \text{Bits}(a_2)$  equals to  $\text{Bits}(a_1 + a_2)$  after some corrections. For instance, suppose a prover wants to prove that the following relations hold for  $M$  inputs and  $S$  outputs:

$$a_i \geq 0, \forall i \in [0, M); \quad \wedge \quad b_i \geq 0, \forall i \in [0, S); \tag{8}$$

$$\sum_{i=0}^{M-1} a_i = \sum_{i=0}^{S-1} b_i; \tag{9}$$

where  $a_i$ 's are input accounts and  $b_i$ 's are output accounts. A balance proof first converts each account into bits,  $\mathbf{a}_i = (a_{i,0}, \dots, a_{i,k-1}) \leftarrow \text{Bits}(a_i)$  and  $\mathbf{b}_i = (b_{i,0}, \dots, b_{i,k-1}) \leftarrow \text{Bits}(b_i)$ , and commits to each  $\mathbf{a}_i$  and  $\mathbf{b}_i$ . Then, it shows 1)  $\mathbf{a}_i$  and  $\mathbf{b}_i$  are binary vectors for Equation (8) and 2) Equation (9) holds such

that:

$$\begin{aligned} \sum_{i=0}^{M-1} a_i &= \sum_{i=0}^{S-1} b_i \iff \sum_{i=0}^{M-1} \sum_{j=0}^{k-1} 2^j a_{i,j} = \sum_{i=0}^{S-1} \sum_{j=0}^{k-1} 2^j b_{i,j} \\ \iff \sum_{i=0}^{S-1} b_{i,j} - \sum_{i=0}^{M-1} a_{i,j} + \tau_j - 2\tau_{j+1} &= 0, \quad \forall j \in [0, k), \end{aligned}$$

where  $\tau_i$ 's are correct values to ensure  $\sum_{i=0}^{S-1} b_{i,j} - \sum_{i=0}^{M-1} a_{i,j} + \tau_j - 2\tau_{j+1} = 0$  holds for all  $j \in [0, k)$  and  $\tau_0 = \tau_k = 0$ .

The balance proof requires additional work to ensure  $\tau_j$ 's are properly generated. In general, the prover needs to ensure  $\tau_i \in [-M + 1, S - 1]$  (Lemma 4.1 in [17]) with range proofs. It is acceptable to embed  $\tau_i$ 's in the binary proof of  $b_{i,j}$ 's when  $M = 1$  and  $S \leq 2$ , as with the Algorithm 8 and 9 in [17]. However, in other cases, the cost of range proofs is not negligible. Taking the state-of-the-art range proof in [14] as an example, the additional range proof requires 3 UMCs (the commitment of  $\tau_i$ 's needs to be included), a  $(k-1) \log(S+M-1)(d/s)$ -size vector (i.e.,  $f_j^{(i)}$ 's in [14] where  $s$  refers to the number of packing slots in [14]), and a  $3md$ -size randomness (i.e.,  $z$  in [14]). Even for a small range, the proof size is prohibitively large as the UMCs and HMCs cannot be batched together. More specifically, under the settings of [17], the range proof costs nearly 200KB, while other parts only cost about 100KB when  $M = 2$  and  $S = 3$ .

Our observation is that the *corrector values* ( $\tau_0, \dots, \tau_k$ ) are unnecessary for balance proofs. To prove Equation (9) holds, one can simply prove

$$\begin{aligned} \sum_{i=0}^{M-1} \sum_{j=0}^{k-1} 2^j a_{i,j} &= \sum_{i=0}^{S-1} \sum_{j=0}^{k-1} 2^j b_{i,j} \\ \iff \sum_{j=0}^{k-1} 2^j \left( \sum_{i=0}^{S-1} b_{i,j} - \sum_{i=0}^{M-1} a_{i,j} \right) &= \sum_{j=0}^{k-1} 2^j c_j = 0, \end{aligned} \tag{10}$$

where  $c_j = \sum_{i=0}^{S-1} b_{i,j} - \sum_{i=0}^{M-1} a_{i,j}$ . The fact behind this idea is that though  $\text{Bits}(a_1) + \text{Bits}(a_2) \neq \text{Bits}(a_1 + a_2)$ , we have  $\langle \text{Bits}(a_1), \mathbf{2}^k \rangle + \langle \text{Bits}(a_2), \mathbf{2}^k \rangle = \langle \text{Bits}(a_1 + a_2), \mathbf{2}^k \rangle$ . Based on this observation, we can fully remove the range proofs of  $\tau_i$ 's as well as the commitments and responses to  $\tau_i$ 's.

Additionally, the prover can also avoid sending the commitment of  $c_j$ 's as it can be derived from the following equation:

$$\text{Com}(c_0, \dots, c_{k-1}; *) = \sum_{i=0}^{S-1} \text{Com}(\mathbf{b}_i; *) - \sum_{i=0}^{M-1} \text{Com}(\mathbf{a}_i; *). \tag{11}$$

Meanwhile, the range proofs of  $c_i$ 's can be avoided when  $\mathbf{a}_i$ 's and  $\mathbf{b}_i$ 's are binary vectors since Equation (11) implies  $c_i \in [-M, S]$ .

The idea of using an inner-product equation to prove balance relations can be generalized to prove the satisfiability of a linear equation (Section 4.1 and

5.1). Besides, we also observe the range of corrector values can be limited to  $\{-1, 0, 1\}$ . As we do not adopt this approach in this paper, we only discuss it in Appendix E.

### 3.2 Binary Proof in Ring Signatures

In most of existing ring signatures [14, 15, 17], a one-out-of-many proof is used to show a prover (signer) knows an opening of a public key  $P_l$  in a public key set  $(P_0, \dots, P_{N-1})$ . The idea for this proof is regarding a public key as a commitment to zero. Thus, by constructing a secret binary sequence  $\delta = (\delta_{l,0}, \dots, \delta_{l,N-1})$  with Hamming weight 1, a prover proves 1)  $\delta$  is well-formed and 2)  $\sum_{i=0}^{N-1} \delta_{l,i} P_i = P_l$  is a commitment to 0. A straightforward solution for the former relation is to use a binary proof to show  $\delta$  is a binary vector and  $\sum_{i=0}^{N-1} f_i = \sum_{i=0}^{N-1} (x\delta_i + a_i) = x$  for a challenge  $x$  and some masking values  $a_i$ 's where  $\sum_{i=0}^{N-1} a_i = 0$ . However, this approach is inefficient as the proof size is  $O(N)$  due to the size of  $\delta$ .

The efficient logarithmic-size ring signatures “compress”  $\delta$  to several shorter delta vectors and allow the verifier to “reconstruct”  $\delta$  with these vectors [14, 15, 17]. Suppose  $N = \beta^k$ . Write  $l = (l_0, \dots, l_{k-1})$  and  $i = (i_0, \dots, i_{k-1})$  as the representations in base  $\beta$  such that  $\delta_{l,i} = \prod_{j=0}^{k-1} \delta_{l_j, i_j}$ . Instead of proving that an  $N$ -size vector  $\delta$  is well-formed, the prover only needs to prove  $k$ -many  $\beta$ -size vectors,  $(\delta_{l_j,0}, \dots, \delta_{l_j,\beta-1})_{j=0}^{k-1}$ , are well-formed, which reduces the proof size to  $O(k\beta)$ .

We have two observations. First, to ensure security, the binary proof requires a larger parameter set than other parts of the proof. This is due to 1) the hardness of the M-SIS problem and 2)  $b(1-b) = 0$  may not hold in  $R_q$  for a smaller  $q$  [17]. Though the binary proof is simple, its larger parameters imply a larger proof size. Motivated by this, we analyze ring signatures and find proving  $\delta$  being a *binary* sequence is redundant. For example, a signer can prove knowing the opening to  $2P_l$  instead of  $P_l$  without sacrificing security. Generally speaking, it is sufficient to relax the one-out-of-many proof by proving that knowing an opening to  $\sum_{i=0}^{N-1} b_i P_i$  in ring signatures, where  $b_i$ 's are short and not all  $b_i$ 's are 0. While reducing binary proof is nice in itself, we would like to highlight that it is particularly important for ring signatures. As “*the binary proof requires a much bigger modulus than (other parts of) the one-out-of-many proof*” [17], avoiding the binary proof fully releases ring signatures from the burden of large parameters. Therefore, instead of running a full one-out-of-many proof, ring signatures can use a much more efficient *linear sum* proof with a small modulus.

Our second observation is the linear sum proof may be difficult to adopt the “compressing” technique in [14, 15, 17] to achieve logarithmic-size ring signatures as there may not exist  $(b_{j,0}, \dots, b_{j,\beta-1})$  such that  $b_i = \prod_{j=0}^{k-1} b_{j,i_j}$  for all  $i \in [0, N)$  and finding such a solution can be very inefficient. This brings us to the idea of adopting “unbalanced” relations as in relaxed proofs: using a stricter relation in proving, but checking the original relation in verifying. For instance, as a linear sum relation is sound for ring signatures and a one-out-of-many relation

is stricter than the linear sum relation, a prover can use  $b_i = \delta_{l,i}$  in the one-out-of-many relation to generate a proof. The verifier checks the linear sum relation of the proof instead of the one-out-of-many relation.

Though our “unbalanced” relation is derived from relaxed relations, the motivations behind are different. In our approach, we start from the *verifier’s* side and show verifying a linear sum proof suffices in ring signatures. To improve the efficiency, we restrict the prover’s relation and require the prover to run under a one-out-of-many relation. The key idea is to find a strict and efficient relation for provers. On the other hand, existing relaxed proofs start from the *prover’s* side and find straightforward soundness proofs do not work. They need to relax the relation on the verifier’s side to overcome the complications. The key is to find a relaxed but sound relation for verifiers. Thus we use the term “unbalanced relations” to distinguish with relaxed relations. We describe the unbalance linear sum proof in Section 4.2 and 5.2

## 4 New Techniques for RingCT Protocols

Based on the ideas in Section 3, we propose two general techniques. The RingCT protocol can be regarded as an application of these techniques.

### 4.1 Linear Equation Satisfiability

**Definition.** Let  $N$  be a positive integer and  $\omega_0, \dots, \omega_{N-1}$  be (public) integers. The linear function is defined as:

$$F(X_0, \dots, X_{N-1}) = \sum_{i=0}^{N-1} \omega_i X_i. \quad (12)$$

The linear equation satisfiability is to prove having the witnesses  $(b_i)_{i=0}^{N-1}$  such that  $F(b_0, \dots, b_{N-1}) = 0$ .

To support  $b_i$ ’s with a wide range in lattice settings, we also use the HMC to commit to the bits of  $b_i$ ’s with  $B_i = \text{Com}(\mathbf{b}_i; *)$ , where  $\mathbf{b}_i$  is the binary representation of  $b_i$ . Thus,  $F(b_0, \dots, b_{N-1})$  can be rewritten as:

$$F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = \sum_{i=0}^{N-1} (\omega_i \cdot \langle \mathbf{2}^k, \mathbf{b}_i \rangle). \quad (13)$$

**Definition 3.** The following defines the linear equation relations, proving  $\mathcal{R}_{LE}$  and relaxed opening  $\mathcal{R}'_{LE}$ :

$$\begin{aligned} \mathcal{R}_{LE}(\mathcal{T}) &= \left\{ \left( (ck, (\omega_i, B_i)_{i=0}^{N-1}), (\mathbf{b}_i, \mathbf{r}_{b,i})_{i=0}^{N-1} \right) : \mathbf{b}_i \in \{0, 1\}^k \wedge \|\mathbf{r}_{b,i}\| \leq \mathcal{T} \right. \\ &\quad \left. \wedge B_i = \text{Com}_{ck}(\mathbf{b}_i; \mathbf{r}_{b,i}) \wedge F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0 \right\}, \\ \mathcal{R}'_{LE}(\widehat{\mathcal{T}}) &= \left\{ \left( (ck, (\omega_i, B_i)_{i=0}^{N-1}), (y, (\mathbf{b}_i, \mathbf{r}_{b,i})_{i=0}^{N-1}) \right) : \mathbf{b}_i \in \{0, 1\}^k \wedge \|\mathbf{r}_{b,i}\| \leq \widehat{\mathcal{T}} \right. \\ &\quad \left. \wedge y \in \mathcal{C}^* \wedge y B_i = \text{Com}_{ck}(\mathbf{b}_i; \mathbf{r}_{b,i}) \wedge F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0 \right\}. \end{aligned}$$

**Inner-product based proof.** Based on the idea discussed in Section 3.1, we propose an inner-product based proof for the linear equation satisfiability. The  $\mathcal{R}_{LE}$  indicates two important relations: 1)  $B_i$ 's are commitments to bits and 2)  $F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0$ . The former one can be proved in a binary proof. For the second relation we can rewrite Equation (13) as

$$\begin{aligned} F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0 &\iff \sum_{i=0}^{N-1} \left( \omega_i \sum_{j=0}^{k-1} 2^j b_{i,j} \right) = 0 \\ &\iff \sum_{j=0}^{k-1} \left( 2^j \cdot \sum_{i=0}^{N-1} \omega_i b_{i,j} \right) = \sum_{j=0}^{k-1} 2^j c_j = 0, \end{aligned} \tag{14}$$

where  $b_{i,j}$  is the  $j$ -th element of  $\mathbf{b}_i$  and  $c_j = \sum_{i=0}^{N-1} \omega_i b_{i,j}$ . Denote  $\mathbf{c} = (c_0, \dots, c_{k-1})$ . The verifier can compute the commitment of  $\mathbf{c}$  with  $B_i$ 's:  $C = \text{Com}(\mathbf{c}; *) = \sum_{i=0}^{N-1} \omega_i B_i$ . Let  $\mathbf{f} = x\mathbf{c} + \mathbf{d}$  with some masking values  $\mathbf{d} = (d_0, \dots, d_{k-1})$  and a challenge  $x$ ,  $D = \text{Com}(\mathbf{d}; *)$ . We have

$$\begin{aligned} \text{Com}(\mathbf{f}; *) &= \text{Com}(x\mathbf{c} + \mathbf{d}; *) = xC + D, \\ \langle \mathbf{f}, \mathbf{2}^k \rangle &= \langle x\mathbf{c} + \mathbf{d}, \mathbf{2}^k \rangle = x\langle \mathbf{c}, \mathbf{2}^k \rangle + \langle \mathbf{d}, \mathbf{2}^k \rangle = \langle \mathbf{d}, \mathbf{2}^k \rangle, \end{aligned} \tag{15}$$

which ensure  $F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0$  holds.

We can further adopt some techniques to reduce the proof size. First, the prover can avoid sending  $\langle \mathbf{d}, \mathbf{2}^k \rangle$  by choosing  $\mathbf{d}$  such that  $\langle \mathbf{d}, \mathbf{2}^k \rangle = 0$  (i.e., setting  $d_0 = -\sum_{j=1}^{k-1} 2^j d_j$ ). The second equation of (15) becomes  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$ . Furthermore, the prover only needs to send  $(f_1, \dots, f_{k-1})$  as  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$ . The verifier computes  $f_0 = -\sum_{j=1}^{k-1} 2^j f_j$ , rebuilds  $\mathbf{f} = (f_0, \dots, f_{k-1})$ , and only checks the first equation in (15).

## 4.2 Ring Signature

**Definition.** Let  $r$  be a private key and  $P_l$  be the corresponding public key in a public key set  $\mathbf{P} = (P_0, \dots, P_{N-1})$  for some  $N \geq 1$  and  $0 \leq l < N$ . The goal of ring signatures is to show the knowledge of a secret key(s) corresponding to a public key(s) in  $\mathbf{P}$ . Based on the idea in Section 3.2, we show that proving the knowledge of an opening of a *short non-zero linear sum* relation of the public keys suffices for ring signatures, i.e., knowing some bounded  $b_i$ 's and an opening to  $\sum_{i=0}^{N-1} b_i P_i$  where at least one  $b_i$  is not zero. This is formally given in Lemma 5.

**Lemma 5.** *In ring signatures, if the commitment scheme is computational hiding and  $\gamma$ -binding, then it is hard to efficiently extract  $(b_i)_{i=0}^{N-1}$  and an opening to  $\sum_{i=0}^{N-1} b_i P_i$  with non-negligible probability, such that  $b_i \in [-\mathcal{B}_{LS}, \mathcal{B}_{LS}]$  and at least one  $b_i$  is not zero, with respect to insider corruption<sup>5</sup> in the random oracle model.*

<sup>5</sup> The attacker can obtain private keys to some public keys with corruption queries. Accordingly, the signature forgery should not include these ‘‘corrupted’’ public keys in its ring.

*Proof.* Assume there exists a PPT adversary  $\mathcal{F}$  that can efficiently extract  $b_i$ 's and a valid opening  $(\mathbf{0}, \mathbf{s})$  of  $\sum_{i=0}^{N-1} b_i P_i$  with non-negligible probability, then we have a collision finder  $\mathcal{A}$  which can break the binding property of the HMC commitment scheme, and solve the M-SIS problem accordingly.

Specifically,  $\mathcal{A}$  samples  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}$  and computes an invalid public key  $P_l = \text{Com}_{ck}(1, 0, \dots, 0; \mathbf{r})$ . Due to the hiding probability of the commitment scheme,  $\mathcal{F}$  cannot distinguish  $P_l$  with other public keys. By calling  $\mathcal{F}$ ,  $\mathcal{A}$  gets  $(b_i)_{i=0}^{N-1}$  and a valid opening  $(\mathbf{0}, \mathbf{s})$  of  $\sum_{i=0}^{N-1} b_i P_i$ . With non-negligible probability, we have  $b_l \neq 0$  since  $\mathcal{F}$  can only make polynomially many registration queries to  $\mathcal{A}$  (calling RKeygen). Then,  $\mathcal{A}$  uses all private keys but  $\mathbf{r}_l$  to compute  $\mathbf{s}' = \mathbf{s} - \sum_{i \neq l} b_i \mathbf{r}_i$ . Since  $b_l \neq 0$ , we have a binding collision for the commitment scheme,  $((b_l, 0, \dots, 0), b_l \mathbf{r})$  and  $(\mathbf{0}, \mathbf{s}')$ . More details about the security reduction is presented in Appendix D.

**Remarks.** The adversary  $\mathcal{A}$  interacts as a collision finder with the HMC challenger and as a ring signature challenger with the  $\mathcal{F}$ . Thus,  $\mathcal{A}$  can access all private keys by calling RKeygen as these key pairs will not help to find a collision without a signature forgery [14, 17, 21]. Besides, since  $b_i$ 's are important to compute the HMC collision, we require  $\mathcal{F}$  also provide  $b_i$ 's along with the forgery  $\mathbf{s}$  (i.e.,  $\mathcal{F}$  here is not exactly as a ring signature forger). More details of  $\mathcal{F}$  extracting  $b_i$ 's are presented in the proof of Theorem 4 (here  $\mathcal{F}$  works as the adversary  $\mathcal{A}$  in Theorem 4).

**Unbalanced Linear Sum Proof.** We further leverage the idea of unbalanced relations in Section 3.2 to propose a logarithmic-size unbalanced linear sum proof, i.e., the prover uses a one-out-of-many relation to run the protocol by setting  $b_i = \delta_{l,i}$  and the verifier checks under a linear sum relation. To ensure at least one  $b_i$  is not zero, the verifier checks whether  $\|\mathbf{b}\| > 0$  in the opening. The unbalanced linear sum relations are defined as follows:

**Definition 4.** *The following defines the unbalanced relations for our unbalanced linear sum proof, proving  $\mathcal{R}_{LS}$  and relaxed opening  $\mathcal{R}'_{LS}$ :*

$$\mathcal{R}_{LS}(\mathcal{T}) = \left\{ ((ck, \mathbf{P}), (l, \mathbf{r})) : l \in [0, N) \wedge \|\mathbf{r}\| \leq \mathcal{T} \wedge P_l = \text{Com}_{ck}(\mathbf{0}; \mathbf{r}) \right\},$$

$$\mathcal{R}'_{LS}(\widehat{\mathcal{T}}_b, \widehat{\mathcal{T}}_r) = \left\{ ((ck, \mathbf{P}), (y, \mathbf{b}, \widehat{\mathbf{r}})) : \|\mathbf{b}\| > 0 \wedge \|\mathbf{b}_i\| \leq \widehat{\mathcal{T}}_b \wedge \|\widehat{\mathbf{r}}\| \leq \widehat{\mathcal{T}}_r \wedge y \sum_{i=0}^{N-1} b_i P_i = \text{Com}_{ck}(\mathbf{0}; \widehat{\mathbf{r}}) \wedge y \text{ is a product of } x_i \in \mathcal{C}^* \right\},$$

In our unbalanced linear sum proofs, the prover first finds and commits to  $k$ -many sequences  $(\delta_{l_j, 0}, \dots, \delta_{l_j, \beta-1})_{j=0}^{k-1}$  which allow the verifier to reconstruct  $\delta$  base on  $\delta_{l,i} = \prod_{j=0}^{k-1} \delta_{l_j, i_j}$  under a one-out-of-many relation. After receiving a challenge  $x$ , the prover's response contains  $f_{j,i} = x \delta_{l_j, i} + a_{j,i}$  with some masking values  $a_{j,i}$ 's. Let  $\delta' = (\delta_{l_0, 0}, \dots, \delta_{l_{k-1}, \beta-1})$ ,  $\mathbf{a} = (a_{0,0}, \dots, a_{k-1, \beta-1})$ , and  $\mathbf{f} = (f_{0,0}, \dots, f_{k-1, \beta-1})$ . To ensure  $\delta'$  is well-formed, the prover shows the following

equations hold:

$$\begin{aligned} \text{Com}(\mathbf{f}; *) &= \text{Com}(x\boldsymbol{\delta}' + \mathbf{a}; *) = xB + A; \\ \sum_{i=0}^{\beta-1} f_{j,i} &= x \sum_{i=0}^{\beta-1} \delta_{l_j,i} + \sum_{i=0}^{\beta-1} a_{j,i} = x + \sum_{i=0}^{\beta-1} a_{j,i}, \quad \forall j \in [0, k). \end{aligned} \quad (16)$$

The second equation ensures at least one element in  $(\delta_{l_j,0}, \dots, \delta_{l_j, \beta-1})$  is not 0 for all  $j$ 's as  $\sum_{i=0}^{\beta-1} f_{j,i} = x + \sum_{i=0}^{\beta-1} a_{j,i}$  implies  $\sum_{i=0}^{\beta-1} \delta_{l_j,i} = 1$ . Moreover, proving  $\boldsymbol{\delta}'$  being “short” is done in the norm check of HMC (presented later in steps 24 and 25 of Protocol 3). Besides, the binary proof for  $\boldsymbol{\delta}'$  is avoided here as we do not require the reconstructed  $\boldsymbol{\delta}$  being a binary vector under the linear sum relation. Furthermore, the second equation is not a necessary condition for the linear sum relation. However, based on the unbalanced relations in Section 3.2, the prover can efficiently show the second equation holds with a one-out-of-many relation. Other steps such as reconstructing  $\boldsymbol{\delta}$  and checking  $\sum_{i=0}^{N-1} \delta_{l_i} P_i$  being a commitment to zero are exactly same as the one-out-of-many proofs in [14, 15, 17], which are presented in Section 5.2.

Similar to the linear equation satisfiability, we also adopt some techniques to reduce our linear sum proof size. First, choosing  $a_{j,i}$ 's such that  $\sum_{i=0}^{\beta-1} a_{j,i} = 0$  can avoid the cost of sending  $\sum_{i=0}^{\beta-1} a_{j,i}$  in Equation (16). Moreover, the prover only needs to send  $(a_{j,i})_{i=1}^{\beta-1}$  which allows the verifier to rebuild  $a_{j,0}$ 's with  $a_{j,0} = -\sum_{i=1}^{\beta-1} a_{j,i}$  for all  $j \in [0, k)$  without further checking the second equation in (16).

## 5 Lattice-based Proofs

We formally describe our balance proof and ring signature for RingCT protocols in lattice settings. In this paper, we separate the two protocols for a clear expression.

### 5.1 Linear Equation Satisfiability

We formally describe our linear equation satisfiability protocol in Protocol 2. Specifically, steps 7 to 11 generate and commit to masking values  $t_{i,j}$ 's for the binary proof of  $\mathbf{b}$ .  $c_j$ 's in Equation (14) are derived in step 12 and their masking values,  $d_j$ 's, are generated in steps 13 and 14 to ensure  $\langle \mathbf{d}, \mathbf{2}^k \rangle = 0$  as discussed in Section 4.1. In steps 17 and 18, the binary proof commitments,  $\text{Com}(\mathbf{b}; *)$  and  $\text{Com}(\mathbf{t} \circ (\mathbf{1} - 2\mathbf{b}); *)$ , are batched together as  $E = \text{Com}(\mathbf{b}, \mathbf{t} \circ (\mathbf{1} - 2\mathbf{b}); *)$ , so does  $F$ .

After receiving the challenge  $x$ , the prover generates the responses based on steps 19 to 30. As  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$  holds, the prover can avoid sending  $f_0$  in steps 21 and 22. In step 24, the randomness for  $\mathbf{c}$  (i.e.,  $\mathbf{r}_c$ ) is derived based on  $\mathbf{r}_{b,i}$ 's since  $c_j = \sum_{i=0}^{N-1} \omega_i b_{i,j}$ .

---

**Protocol 2** Linear Equation Satisfiability
 

---

$$\mathcal{P}_{LE}(ck, (\omega_i, B_i)_{i=0}^{N-1}, (\mathbf{b}_i, \mathbf{r}_{b,i})_{i=0}^{N-1}) \quad \mathcal{V}_{LE}(ck, (\omega_i, B_i)_{i=0}^{N-1})$$

- 1:  $\boldsymbol{\omega} = (\omega_0, \dots, \omega_{N-1})$
  - 2:  $T_1 = p\sqrt{wkN}$
  - 3:  $T_2 = \max(-\sum_{\omega_i < 0} \omega_i, \sum_{\omega_i > 0} \omega_i)p\sqrt{wk}$
  - 4:  $T_3 = \mathcal{B}wp\sqrt{md}(\|\boldsymbol{\omega}\|_1^2 + N + 1)$
  - 5:  $\mathbf{r}_b \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$
  - 6:  $\mathbf{r}_t, \mathbf{r}_d \leftarrow D_{\phi_3 T_3}^{md}$
  - 7: **for**  $i = 0$  to  $N - 1$  **do**
  - 8:    $t_{i,0}, \dots, t_{i,k-1} \leftarrow D_{\phi_1 T_1}^d$
  - 9:    $\mathbf{r}_{t,i} \leftarrow D_{\phi_3 T_3}^{md}$
  - 10:    $G_i = \text{Com}_{ck}(t_{i,0}, \dots, t_{i,k-1}; \mathbf{r}_{t,i})$
  - 11: **end for**
  - 12:  $c_j = \sum_{i=0}^{N-1} \omega_i b_{i,j}, \forall j \in [0, k)$
  - 13:  $d_1, \dots, d_{k-1} \leftarrow D_{\phi_2 T_2}^d$
  - 14:  $d_0 = -\sum_{j=1}^{k-1} 2^j \cdot d_j$
  - 15:  $\mathbf{b} = (b_{i,j})_{i=0, j=0}^{N-1, k-1}, \mathbf{t} = (t_{i,j})_{i=0, j=0}^{N-1, k-1}, \mathbf{d} = (d_i)_{i=0}^{k-1}$
  - 16:  $D = \text{Com}_{ck}(\mathbf{d}; \mathbf{r}_d)$
  - 17:  $E = \text{Com}_{ck}(\mathbf{b}, \mathbf{t} \circ (\mathbf{1} - 2\mathbf{b}); \mathbf{r}_b)$
  - 18:  $F = \text{Com}_{ck}(\mathbf{t}, -\mathbf{t} \circ \mathbf{t}; \mathbf{r}_t)$
- $$\begin{array}{c} \xrightarrow{D, E, F, (G_i)_{i=0}^{N-1}} \\ \xleftarrow{x} \end{array} \quad x \leftarrow \mathcal{C}$$
- 19:  $\mathbf{g} = x\mathbf{b} + \mathbf{t}$
  - 20:  $\text{Rej}(\mathbf{g}, x\mathbf{b}, \phi_1, T_1)$
  - 21:  $\mathbf{c}_1 = (c_j)_{j=1}^{k-1}, \mathbf{d}_1 = (d_j)_{j=1}^{k-1}$
  - 22:  $\mathbf{f}_1 = x\mathbf{c}_1 + \mathbf{d}_1$
  - 23:  $\text{Rej}(\mathbf{f}_1, x\mathbf{c}_1, \phi_2, T_2)$
  - 24:  $\mathbf{r}_c = \sum_{i=0}^{N-1} \omega_i \mathbf{r}_{b,i}$
  - 25:  $\mathbf{z} = x\mathbf{r}_c + \mathbf{r}_d$
  - 26:  $\mathbf{z}_g = x\mathbf{r}_b + \mathbf{r}_t$
  - 27: **for**  $i = 0$  to  $N - 1$  **do**
  - 28:    $\mathbf{z}_{b,i} = x\mathbf{r}_{b,i} + \mathbf{r}_{t,i}$
  - 29: **end for**
  - 30:  $\text{Rej}((\mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1}), x(\mathbf{r}_c, \mathbf{r}_b, (\mathbf{r}_{b,i})_{i=0}^{N-1}), \phi_3, T_3)$
- $$\begin{array}{c} \xrightarrow{\mathbf{f}_1, \mathbf{g}, \mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1}} \\ \end{array}$$
- 31:  $\mathbf{g} = (g_{0,0}, \dots, g_{S-1, k-1})$
  - 32:  $\mathbf{g}_i = (g_{i,0}, \dots, g_{i, k-1}), \forall i$
  - 33:  $\mathbf{h} = (g_{i,j}(x - g_{i,j}))_{i=0, j=0}^{N-1, k-1}$
  - 34:  $\mathbf{f}_1 = (f_1, \dots, f_{k-1})$
  - 35:  $f_0 = -\sum_{j=1}^{k-1} 2^j \cdot f_j$
  - 36:  $\mathbf{f} = (f_0, \dots, f_{k-1})$
  - 37:  $C = \sum_{i=0}^{N-1} \omega_i B_i$
  - 38:  $\|g_{i,j}\| \stackrel{?}{\leq} 2\phi_1 T_1 \sqrt{d}, \quad \forall i, j$
  - 39:  $\|f_j\| \stackrel{?}{\leq} 2\phi_2 T_2 \sqrt{d}, \quad \forall j \neq 0$
  - 40:  $\|f_0\| \stackrel{?}{\leq} 2\phi_2 T_2 \sqrt{2^k d}$
  - 41:  $\|\mathbf{z}\|, \|\mathbf{z}_g\|, \|\mathbf{z}_{b,i}\| \stackrel{?}{\leq} 2\phi_3 T_3 \sqrt{md}, \forall i$
  - 42:  $x\mathbf{C} + D \stackrel{?}{=} \text{Com}_{ck}(\mathbf{f}; \mathbf{z})$
  - 43:  $x\mathbf{E} + F \stackrel{?}{=} \text{Com}_{ck}(\mathbf{g}, \mathbf{h}; \mathbf{z}_g)$
  - 44:  $x\mathbf{B}_i + G_i \stackrel{?}{=} \text{Com}_{ck}(\mathbf{g}_i; \mathbf{z}_{b,i}), \forall i$
-

Finally, the verifier generates  $f_0$  in step 35 to ensure  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$  holds (i.e.,  $F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0$ ). A trick to avoid the overflow of  $\sum_{j=1}^{k-1} 2^j \cdot f_j$  under a small  $q$  is to compute  $f_0$  under  $R$  instead of  $R_q$  and return false if  $f_0$  is not in  $R_q$ . The commitment of  $\mathbf{c}$  (step 37) is derived based on  $B_i$ 's. Step 42 ensures  $f_i$ 's are properly generated from  $c_i$ 's and the last two steps ensure  $\mathbf{b}_i$ 's are binary vectors.

**Theorem 1.** *Let  $\gamma_{LE} = 4\phi_3 md\mathcal{B}wp(\|\boldsymbol{\omega}\|_1^2 + N + 1)^{1/2}$  and the HMC is hiding and  $\gamma_{LE}$ -binding. Protocol 2 has 3-special soundness for relations  $\mathcal{R}_{LE}(\mathcal{B}\sqrt{md})$  and  $\mathcal{R}'_{LE}(\gamma_{bal})$  with a completeness error  $1 - 1/(\mu(\phi_1)\mu(\phi_2)\mu(\phi_3))$  defined in Lemma 8.*

The proof for Theorem 1 is given in Appendix B.

## 5.2 Unbalanced Linear Sum Proof

We formally describe our unbalanced linear sum proof protocol. Based on the description of Section 4.2, the prover needs to show 1)  $(\delta_{l_j,0}, \dots, \delta_{l_j,\beta-1})$ 's are short non-zero vectors and are properly committed and 2)  $\delta_{l,i}$ 's can be constructed with  $\delta_{l,i} = \prod_{j=0}^{k-1} \delta_{l_j,i_j}$  such that  $\sum_{i=0}^{N-1} \delta_{l,i} P_i$  being a commitment to zero. The first relation is discussed in Section 4.2 which implies  $\boldsymbol{\delta} = (\delta_{l,0}, \dots, \delta_{l,N-1})$  being a short and non-zero vector. Here we focus on the second relation.

After receiving a challenge  $x$ , the prover's response contains  $f_{j,i} = x\delta_{l_j,i} + a_{j,i}$  with some masking values  $a_{j,i}$ 's. To rebuild  $\delta_{l,i}$ 's, the verifier computes the product  $p_i(x) = \prod_{j=0}^{k-1} f_{j,i_j}$ :

$$\begin{aligned} p_i(x) &= \prod_{j=0}^{k-1} f_{j,i_j} = \prod_{j=0}^{k-1} (x\delta_{l_j,i_j} + a_{j,i_j}) \\ &= x^k \cdot \prod_{j=0}^{k-1} \delta_{l_j,i_j} + \sum_{j=0}^{k-1} p_{i,j} \cdot x^j = \delta_{l,i} x^k + \sum_{j=0}^{k-1} p_{i,j} x^j, \end{aligned} \tag{17}$$

where  $p_{i,j}$ 's are functions of  $\delta_{l_j,i_j}$ 's (i.e.,  $l$ ) and  $a_{j,i}$ 's. Equation (17) holds for all  $i \in [0, N)$ . As  $p_{i,j}$ 's are independent of  $x$ , the prover can pre-compute  $p_{i,j}$ 's and send  $E_j = \sum_{i=0}^{N-1} p_{i,j} P_i$  to allow the verifier to cancel out the coefficients of the terms  $1, x, \dots, x^{k-1}$  before receiving  $x$  (the randomness is omitted here for simplicity). For  $x^k$  part, it can be set to the prover's public key  $P_l$  with  $\sum_{i=0}^{N-1} \delta_{l,i} P_i$ . Our unbalanced linear sum proof is formally described in Protocol 3.

In Protocol 3, steps 4 to 7 generate the masking values  $a_{j,i}$ 's for  $\delta_{l_j,i}$ 's and ensure  $\sum_{i=0}^{\beta-1} a_{j,i} = 0$  (which further ensures  $\sum_{i=0}^{\beta-1} (x\delta_{l_j,i} + a_{j,i}) = x$ ). The  $p_{i,j}$ 's in steps 11 and 14 are derived based on Equation (17).

Upon receiving the challenge  $x$ , the prover generates the responses  $\mathbf{f}_1, \mathbf{z}_b$ , and  $\mathbf{z}_r$ . For  $\mathbf{f}$ , the prover can avoid sending  $f_{j,0}$ 's as  $\sum_{i=0}^{\beta-1} f_{j,i} = x$  holds. In step 21,  $\mathbf{z}_r$  is the response to randomness in  $P_l$  and  $E_j$ 's based on Equation (17). As  $\boldsymbol{\rho}_0$

is sampled from  $D_{\phi_2 T_2}^{md}$  and other  $\rho_j$ 's and  $\mathbf{r}$  are sampled from  $\{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$ ,  $\rho_0$  is the masking vector for  $x^k \mathbf{r} - \sum_{j=1}^{k-1} x^j \rho_j$  (step 21).

Finally, the verifier computes  $f_{j,0} = x - \sum_{i=1}^{\beta-1} f_{j,i}$  for all  $j \in [0, k)$  as  $\sum_{i=0}^{\beta-1} f_{j,i} = x$ , which ensures  $\sum_{i=0}^{\beta-1} \delta_{l_j,i} = 1$  (and further ensures at least one element in  $(\delta_{l_j,0}, \dots, \delta_{l_j,\beta-1})$  is not 0 for all  $j$ 's). The last two steps ensure that  $\sum_{i=0}^{N-1} \delta_{l_i} P_i$  is a commitment to 0 as discussed in Section 4.2.

**Theorem 2.** *Let  $\gamma_{LS} = (4\phi_1 \sqrt{k\beta})^k d^{k-\frac{1}{2}}$ ,  $\gamma'_{LS} = (k+1)2^{\kappa'+2} \sqrt{2}\phi_2 \mathcal{B} m d^2 w^\kappa p^{\kappa+1}$  for  $\kappa = k(k+1)/2$  and  $\kappa' = k(k-1)/2$ , the HMC is hiding and  $\gamma_{LS}$ -binding. Protocol 3 has  $(k+1)$ -special soundness for relations  $\mathcal{R}_{LS}(\mathcal{B}\sqrt{md})$  and  $\mathcal{R}'_{LS}(\gamma_{LS}, \gamma'_{LS})$  with a completeness error  $1 - 1/(\mu(\phi_1)\mu(\phi_2))$  defined in Lemma 8.*

The proof for Theorem 2 is given in Appendix C.

## 6 Efficient ZKPs for RingCT

As applications of our techniques, we show how to build balance proofs and ring signatures for RingCT protocols.

### 6.1 Non-Interactive Balance Proof

Based on Protocol 2, we design an efficient non-interactive balance proof for RingCT protocols. Consider the case in Section 3.1 with  $M$  input accounts  $(a_i)_{i=0}^{M-1}$  and  $S$  output accounts  $(b_i)_{i=0}^{S-1}$ . The balance proof is a special case of linear equation satisfiability, where  $N = S + M$ ,  $(\omega_0, \dots, \omega_{S-1}) = (1, \dots, 1)$ , and  $(\omega_S, \dots, \omega_{S+M-1}) = (-1, \dots, -1)$ . Accordingly, Equation (12) can be expressed as  $F(a_0, \dots, a_{M-1}, b_0, \dots, b_{S-1}) = \sum_{i=0}^{S-1} b_i - \sum_{i=0}^{M-1} a_i$ .

Let  $\mathbf{CN}_{in} = (A_i)_{i=0}^{M-1}$  and  $\mathbf{CN}_{out} = (B_i)_{i=0}^{S-1}$  be the sets of input and output coins respectively (i.e., commitments to  $\mathbf{a}_i$ 's and  $\mathbf{b}_i$ 's),  $\mathbf{CNK}_{in} = (r_{a,i})_{i=0}^{M-1}$  and  $\mathbf{CNK}_{out} = (r_{b,i})_{i=0}^{S-1}$  be the sets of input and output coin keys (i.e. randomness). Denote the initial commitments in Protocol 2 as  $\mathbf{CMT} = (D, E, F, (G_i)_{i=0}^{S-1})$ , the prover's response as  $\mathbf{RSP} = (\mathbf{f}_1, \mathbf{g}, \mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{S-1})$ , and  $\mathbf{CMT}^* = E$ . The most important functions in the balance proof part of RingCT protocols are defined as follows:

- **Setup**( $1^\lambda$ ): Run  $\mathbf{G} \leftarrow \mathbf{CKeygen}$  and set  $ck = \mathbf{G}$ . Choose a hash function  $H : \{0, 1\}^* \rightarrow \mathcal{C}$ . Return  $pp = (ck, H)$ .
- **Mint**( $pp, v$ ): Sample  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$  and compute  $(v_0, \dots, v_{k-1}) \leftarrow \mathbf{Bits}(v)$ ,  $B = \text{Com}_{ck}(\mathbf{v}; \mathbf{r})$ . Return  $(\mathbf{cn}, \mathbf{cnk}) = (B, \mathbf{r})$ .
- **Spend**( $(a_i)_{i=0}^{M-1}, (b_i)_{i=0}^{S-1}, pp, \mathbf{CN}_{in}, \mathbf{CNK}_{in}$ ): Parse  $\mathbf{CN}_{in} = (A_i)_{i=0}^{M-1}$  and  $\mathbf{CNK}_{in} = (r_{a,i})_{i=0}^{M-1}$ . Set  $\mathbf{a}_i \leftarrow \mathbf{Bits}(a_i)$  for  $i \in [0, M)$  and  $\mathbf{b}_i \leftarrow \mathbf{Bits}(b_i)$  for  $i \in [0, S)$ . Call  $\mathbf{Mint}(pp, b_i) = (\mathbf{cn}_i, \mathbf{cnk}_i) = (B_i, r_{b,i})$  for  $i \in [0, S)$  to mint coins for output accounts. Set  $\mathbf{CN}_{out} = (\mathbf{cn}_i)_{i=0}^{S-1}$  and  $\mathbf{CNK}_{out} = (\mathbf{cnk}_i)_{i=0}^{S-1}$ . Proceed as follows:

---

**Protocol 3** Unbalanced Linear Sum Proof
 

---

$\mathcal{P}_{LS}(ck, \mathbf{P}, (l, \mathbf{r}))$	$\mathcal{V}_{LS}(ck, \mathbf{P})$
1: $T_1 = p\sqrt{kw}$ , $T_2 = (wp)^k \mathcal{B}\sqrt{2md}$	
2: $\mathbf{r}_a \leftarrow D_{\phi_2 T_2}^{md}$	
3: $\mathbf{r}_b \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$	
4: <b>for</b> $j = 0$ to $k - 1$ <b>do</b>	
5: $a_{j,1}, \dots, a_{j,\beta-1} \leftarrow D_{\phi_1 T_1}^d$	
6: $a_{j,0} = -\sum_{i=1}^{\beta-1} a_{j,i}$	
7: <b>end for</b>	
8: $\boldsymbol{\delta} = (\delta_{l_0,0}, \dots, \delta_{l_{k-1},\beta-1})$	
9: $\mathbf{a} = (a_{0,0}, \dots, a_{k-1,\beta-1})$	
10: $\boldsymbol{\rho}_0 \leftarrow D_{\phi_2 T_2}^{md}$	
11: $E_0 = \sum_{i=0}^{N-1} p_{i,0} P_i + \text{Com}_{ck}(\mathbf{0}; \boldsymbol{\rho}_0)$	
12: <b>for</b> $j = 1$ to $k - 1$ <b>do</b>	
13: $\boldsymbol{\rho}_j \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$	
14: $E_j = \sum_{i=0}^{N-1} p_{i,j} P_i + \text{Com}_{ck}(\mathbf{0}; \boldsymbol{\rho}_j)$	
15: <b>end for</b>	
16: $B = \text{Com}_{ck}(\boldsymbol{\delta}; \mathbf{r}_b)$ , $A = \text{Com}_{ck}(\mathbf{a}; \mathbf{r}_a)$	
$A, B, (E_j)_{j=0}^{k-1}$	
$\xrightarrow{x}$	$x \leftarrow \mathcal{C}$
17: $\boldsymbol{\delta}_1 = (\delta_{l_0,1}, \dots, \delta_{l_{k-1},\beta-1})$	
18: $\mathbf{a}_1 = (a_{0,1}, \dots, a_{k-1,\beta-1})$	
19: $\mathbf{f}_1 = x\boldsymbol{\delta}_1 + \mathbf{a}_1$	
20: $\text{Rej}(\mathbf{f}_1, x\boldsymbol{\delta}_1, \phi_1, T_1)$	
21: $\mathbf{z}_b = x\mathbf{r}_b + \mathbf{r}_a$ , $\mathbf{z}_r = x^k \mathbf{r} - \sum_{j=0}^{k-1} x^j \boldsymbol{\rho}_j$	
22: $\text{Rej}((\mathbf{z}_b, \mathbf{z}_r), (x\mathbf{r}_b, x^k \mathbf{r} - \sum_{j=1}^{k-1} x^j \boldsymbol{\rho}_j), \phi_2, T_2)$	
$\mathbf{f}_1, \mathbf{z}_b, \mathbf{z}_r$	
$\xrightarrow{\quad}$	
23: $f_{j,0} = x - \sum_{i=1}^{\beta-1} f_{j,i}, \forall j \in [0, k)$	
24: $\ f_{j,i}\  \stackrel{?}{\leq} 2\phi_1 T_1 \sqrt{d}, \quad \forall j, \forall i \neq 0$	
25: $\ f_{j,0}\  \stackrel{?}{\leq} 2\phi_1 T_1 \sqrt{\beta d}, \forall j \in [0, k)$	
26: $\ \mathbf{z}_b\ , \ \mathbf{z}_r\  \stackrel{?}{\leq} 2\phi_2 T_2 \sqrt{md}$	
27: $\mathbf{f} = (f_{0,0}, \dots, f_{k-1,\beta-1})$	
28: $x\mathbf{B} + \mathbf{A} \stackrel{?}{=} \text{Com}_{ck}(\mathbf{f}; \mathbf{z}_b)$	
29: $\sum_{i=0}^{N-1} (\prod_{j=0}^{k-1} f_{j,i_j}) P_i - \sum_{j=0}^{k-1} E_j x^j \stackrel{?}{=} \text{Com}_{ck}(\mathbf{0}; \mathbf{z}_r)$	

---

1. Run  $\mathcal{P}_{LE}(ck, ((1, B_i)_{i=0}^{S-1}, (-1, A_i)_{i=0}^{M-1}), ((\mathbf{b}_i, \mathbf{r}_{b,i})_{i=0}^{S-1}, (\mathbf{a}_i, \mathbf{r}_{a,i})_{i=0}^{S-1}))$  to generate CMT based on the first 18 steps<sup>6</sup> of Protocol 2.
2. Compute  $x = H(ck, (A_i)_{i=0}^{M-1}, (B_i)_{i=0}^{S-1}, \text{CMT})$ .
3. Compute RSP by running the remaining steps of  $\mathcal{P}_{LE}$ .
4. Return  $\text{CN}_{out}$  and  $\pi = (\text{CMT}^*, x, \text{RSP})$ .

• **Verify**( $\text{CN}_{in}, \text{CN}_{out}, \pi, pp$ ): Parse  $\text{CN}_{in} = (A_i)_{i=0}^{M-1}$ ,  $\text{CN}_{out} = (B_i)_{i=0}^{S-1}$ ,  $\pi = (\text{CMT}^*, x, \text{RSP})$ . Proceed as follows:

1. Compute  $C, D, F$ , and  $(G_i)_{i=0}^{S-1}$  based on step 37, 42, 43, and 44 of Protocol 2 and set  $\text{CMT} = (D, E, F, (G_i)_{i=0}^{S-1})$ .
2. Return 0 if  $x \neq H(ck, (A_i)_{i=0}^{M-1}, (B_i)_{i=0}^{S-1}, \text{CMT})$ .
3. Return the output of  $\mathcal{V}_{LE}(ck, ((1, B_i)_{i=0}^{S-1}, (-1, A_i)_{i=0}^{M-1}))$  with  $(\text{CMT}, x, \text{RSP})$ .

Notice that this non-interactive balance proof does not ensure anonymity. It can be extended to an anonymous RingCT protocol with the (linkable) ring signature scheme (described in Section 8). As other functions such as **AccountGen** and **CheckAct** are relatively simple and have been discussed in details in [17], we omit these functions here.

**Theorem 3.** *Let  $\gamma_{LE} = 4\phi_3 md \mathcal{B}wp(S+M+1)$ , and the HMC is hiding and  $\gamma_{LE}$ -binding. The balance proof has 3-special soundness for relations  $\mathcal{R}_{LE}(\mathcal{B}\sqrt{md})$  and  $\mathcal{R}'_{LE}(\gamma_{bal})$  with a completeness error  $1 - 1/(\mu(\phi_1)\mu(\phi_2)\mu(\phi_3))$  defined in Lemma 8.*

*Proof.* Considering  $N = S+M$ ,  $(\omega_0, \dots, \omega_{S-1}) = (1, \dots, 1)$ , and  $(\omega_S, \dots, \omega_{S+M-1}) = (-1, \dots, -1)$ , we have  $\|\omega\|_1 = S+M \geq 1$ . Equation (24) can be further simplified as:

$$\mathcal{B}wp\sqrt{md(\|\omega\|_1^2 + N + 1)} \leq \mathcal{B}wp(S+M+1)\sqrt{md} = T_3. \quad (18)$$

Thus, we have  $\|\mathbf{z}\|, \|\mathbf{z}_g\|, (\|\mathbf{z}_{b,i}\|)_{i=0}^{N-1} \leq 2(\phi_3 T_3)\sqrt{md}$  and  $\gamma_{LE} = 4\phi_3 md \mathcal{B}wp(S+M+1)$ .

Other parts can be derived directly from Theorem 1.

## 6.2 Ring Signature

Protocol 3 can be used to construct an efficient ring signature scheme. Let  $M$  be the message to be signed, the initial commitment in Protocol 3 be  $\text{CMT} = (A, B, (E_j)_{j=0}^{k-1})$ , and the prover's response be  $\text{RSP} = (\mathbf{f}_1, \mathbf{z}_b, \mathbf{z}_r)$ . Denote  $\text{CMT}^* = (B, (E_j)_{j=1}^{k-1})$ . The ring signature is defined as follows:

• **RSetup**( $1^\lambda$ ): Run  $\mathbf{G} \leftarrow \text{CKeygen}$  and set  $ck = \mathbf{G}$ . Choose a hash function  $H : \{0, 1\}^* \rightarrow \mathcal{C}$ . Return  $pp = (ck, H)$ .

• **RKeygen**( $pp$ ): Sample  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$  and compute  $P = \text{Com}_{ck}(\mathbf{0}; \mathbf{r})$ . Return  $(pk, sk) = (P, \mathbf{r})$ .

• **RSign**( $M, \mathbf{P}, pp, sk$ ): Parse  $\mathbf{P} = (P_0, \dots, P_{N-1})$  and  $P_l = \text{Com}_{ck}(\mathbf{0}; sk)$  for  $l \in [0, N)$ . Proceed as follows:

<sup>6</sup> In existing anonymous cryptocurrency implementations, binary proofs for inputs  $\mathbf{a}_i$ 's can be reduced as they have been verified as output accounts in previous transactions.

1. Generate CMT by running  $\mathcal{P}_{LS}(ck, \mathbf{P}, (l, \mathbf{r}))$ , step 1 to 16 in Protocol 3.
2. Compute  $x = H(ck, M, \mathbf{P}, \text{CMT})$ .
3. Compute RSP by running the remaining steps of  $\mathcal{P}_{LS}$ .
4. Return  $\pi = (\text{CMT}^*, x, \text{RSP})$ .

• **RVerify**( $M, \mathbf{P}, \pi, pp$ ): Parse  $\mathbf{P} = (P_0, \dots, P_{N-1})$ ,  $\pi = (\text{CMT}^*, x, \text{RSP})$ , and  $\text{CMT}^* = (B, (E_j)_{j=1}^{k-1})$ . Proceed as follows:

1. Compute  $A$  and  $E_0$  based on step 28 and 29 of Protocol 3 and set  $\text{CMT} = (A, B, (E_j)_{j=0}^{k-1})$ .
2. Return 0 if  $x \neq H(ck, M, \mathbf{P}, \text{CMT})$ .
3. Return the output of  $\mathcal{V}_{LS}(ck, \mathbf{P})$  with  $(\text{CMT}, x, \text{RSP})$ .

The correctness and anonymity of the ring signature can be derived directly from the completeness and SHVZK of Protocol 3. The unforgeability of the ring signature is formally described as follows:

**Theorem 4.** *If the commitment scheme is computational hiding and  $\gamma$ -binding, then the ring signature scheme described above is unforgeable with respect to insider corruption in the random oracle model.*

*Proof.* Assume there exists a PPT adversary  $\mathcal{F}$  that can efficiently forge a ring signature with non-negligible probability, we have an adversary  $\mathcal{A}$  which can break the binding property of the commitment scheme, and solve the M-SIS problem accordingly.

$\mathcal{A}$  samples  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}$  and computes an invalid public key  $pk_l = \text{Com}_{ck}(1, 0, \dots, 0; \mathbf{r})$ . Due to the hiding probability of the commitment scheme,  $\mathcal{F}$  cannot distinguish  $pk_l$  with other public keys. Then,  $\mathcal{A}$  runs  $\mathcal{F}$  for  $(k+1)$  times to get  $(k+1)$  forgeries with distinct challenges and a same  $\text{CMT}^*$  part based on the forking lemma ( $pk_l$  is not corrupted). Furthermore,  $\mathcal{A}$  reconstructs CMT and runs the extractor of Protocol 3 with the  $(k+1)$  forgeries to get valid  $b'_i = y^k b_i$  for  $i \in [0, N)$  and a valid opening  $(\mathbf{0}, \mathbf{s})$  of  $y \sum_{i=0}^{N-1} b_i \cdot pk_i$  for some public keys. Thus, we have proper  $b'_i$ 's and a valid opening  $(\mathbf{0}, y^{k-1} \mathbf{s})$  of  $\sum_{i=0}^{N-1} b'_i \cdot pk_i$ . Based on Lemma 5, we have a collision for the commitment scheme,  $((b'_i, 0, \dots, 0), b'_i \mathbf{r})$  and  $(\mathbf{0}, y^{k-1} \mathbf{s} - \sum_{i \neq l} b'_i \mathbf{r}_i)$  as  $(b'_l, 0, \dots, 0) \neq \mathbf{0}$  ( $\mathbf{r}_i$ 's are the private keys as the output of  $\text{Corrupt}(i)$  in the proof of Lemma 5). More details about the security reduction is presented in Appendix D.

## 7 Evaluation

**Implementation.** To evaluate the performance of the proposed proofs, we give a reference implementation of both MatRiCT [17] and our approaches in Golang [19]. The underlying polynomial ring operations are implemented with LAGO [24]<sup>7</sup>. For the linear equation satisfiability, we only implement the balance proof version (i.e.,  $\omega_i$ 's are fixed in our code) to compare with the balance

<sup>7</sup> We also found a bug in MulPoly function of LAGO. Please refer to our repository [19] for more details.

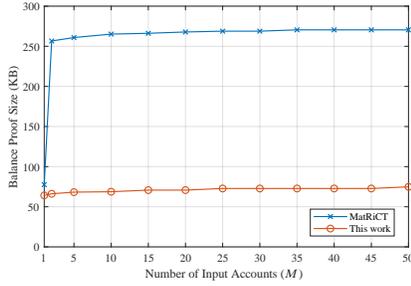


Fig. 1: Balance proof size growth with the number of input accounts ( $M$ ) when  $S = 1$ .

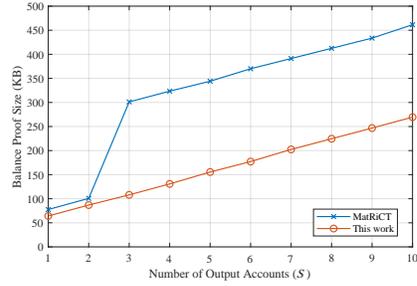


Fig. 2: Balance proof size growth with the number of output accounts ( $S$ ) when  $M = 1$ .

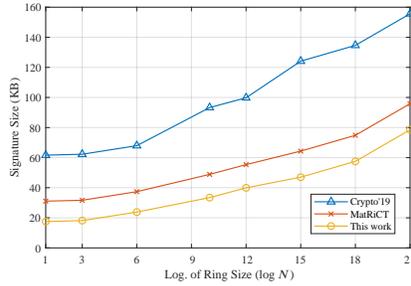


Fig. 3: Ring signature size. The size of MatRiCT does not include the cost of serial numbers for fairness.

proof in MatRiCT. The code of MatRiCT and our work is published in [19]. All experiments are performed on a personal laptop equipped with Intel i7-8750H 2.20GHz CPU and 8GB memory.

**Proof size: balance proof.** We first evaluate the performance of our balance proof. Referring to [17], we consider the scenario that requires 64-bit precision for amounts (i.e.,  $k = 64$ ) and set the parameters as:  $\mathcal{B} = 1$ ,  $(d, w, p) = (64, 56, 8)$ ,  $q = (2^{27} - 2^{21} + 1) \cdot (2^{26} - 2^{12} + 1) \approx 2^{53}$ ,  $(n, m) = (32, 65)$ , and  $\phi_1 = \phi_2 = \phi_3 = 15$ . These parameters are chosen based on a “root Hermite factor” of  $\delta \approx 1.0045$  for both M-LWE and M-SIS, and ensure 128-bit security based on the “LWE estimator” [1]. More details are discussed in [14, 17].

As the Algorithm 8 and 9 in [17] only deal with  $M = 1$  and  $S \leq 2$ , we need to include an additional range proof in MatRiCT for other cases. However, MatRiCT does no specified range proof approaches in [17]. According to the discussion in Section 3.1, we use the state-of-the-art range proof in [14] to evaluate the performance of MatRiCT (the number of slot in CRT packing is set to 16 as with [14]). For  $M = 1$  and  $S \leq 2$  cases, we follow algorithms 8 and 9 in [17] as the implementation of MatRiCT.

First, we show the balance proof size growth with the number of input accounts in Figure 1. Different from the result in [17], our result shows the proof

size is relatively small and does not scale linearly with  $M$ . It is because [17] takes  $NM$  input accounts for anonymity ( $N$  is the set size as in ring signatures). Thus, other  $(N - 1)M$  hiding accounts contribute to a great part of the proof size, which scales linearly with the size in [17]. While in our experiment, we do not consider anonymity in balance proofs. Furthermore, there is a clear burst in MatRiCT when  $M = 2$ . It is due to the additional range proofs for corrector values. The burst also indicates the cost of range proofs is prohibitively large for real-world implementations. Besides, the proof size does not increase much with  $M$  except for  $M = 1$ . For some  $M$ , e.g.  $M \in [30, 40]$ , the size remains the same. This is an expected result as  $M$  contributes to the size of each element in  $\mathbf{g}$ ,  $\mathbf{z}_b$ , and  $\mathbf{z}_r$ , instead of the length of these vectors. Finally, our balance proof can reduce about 15% size of MatriCT when  $M = 1$  and more than 70% in other cases.

Second, we present the balance proof size growth with the number of output accounts in Figure 2. As discussed above, the burst of MatRiCT is caused by range proofs. When  $S > 2$ , the proof size scales linearly with  $S$  due to the cost of  $(\mathbf{z}_{b,i})_{i=0}^{S-1}$ . As  $S$  also contributes to the size of vector elements, the growth is not exactly linear. Generally speaking, our approach can reduce 15% proof size of MatRiCT when  $S < 2$  and up to 60% for other cases.

**Proof size: ring signature.** We further evaluate the performance of our ring signature, and compare with Crypto’19 [14] and MatRiCT [17]. We use the same settings in [17] with two sets of parameters:  $(\hat{n}, \hat{m}) = (32, 65)$ ,  $\hat{q} = (2^{27} - 2^{21} + 1) \cdot (2^{26} - 2^{12} + 1) \approx 2^{53}$  for the binary proof part; and  $(n, m) = (18, 38)$ ,  $q = 2^{31} - 2^{18} + 2^3 + 1 \approx 2^{31}$  for other parts. Other settings for the two parts are same (i.e.,  $(d, w, p) = (64, 56, 8)$ ). Please note that as our unbalanced linear sum proof avoids the binary proofs, only the smaller parameters,  $n$ ,  $m$ , and  $q$ , affect the performance.

The signature size growth with the logarithmic ring size  $\log(N)$  is depicted in Figure 3. The result of Crypto’19 is not as “smooth” as that in [14]. It is caused by the parameters we used are different from short infinity norm challenges in [14]. Besides, our result also shows that MatRiCT does not improve much of Crypto’19, which is different from the results in [17]. This is mainly caused by the parameter settings, as  $d$  and  $q$  in [14] are much larger than those in [17]. Since MatRiCT uses the same blueprint in Crypto’19, Crypto’19 is also improved under MatRiCT settings. Moreover, in our ring signature approach, as we avoid the cost of a binary proof, the sizes of a commitment and  $\mathbf{z}_b, \mathbf{z}_r$  elements are much smaller. A further observation is that all approaches do not scale logarithmically in  $N$ . This is due to the growth of element size. Comparing with existing state-of-the-art approaches, our ring signature is the most efficient which can reduce about 50% and 20% of the signature size in Crypto’19 and MatRiCT respectively.

**Proving/verification time.** Finally, we compare the proving and verification time of our approaches with MatRiCT [17]. As we explained earlier, the balance proof in MatRiCT only works when  $M = 1$  and  $S \leq 2$ , we only compare the performance in two cases,  $(M, S) = (1, 1)$  and  $(M, S) = (1, 2)$ . The results are depicted in Figure 4. Our inner-product based approach reduces nearly 30%

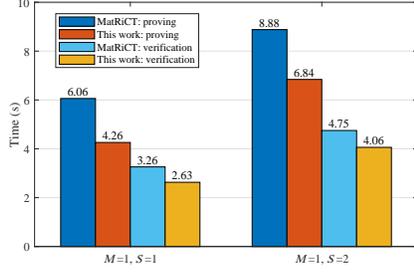


Fig. 4: Time cost of balance proofs.

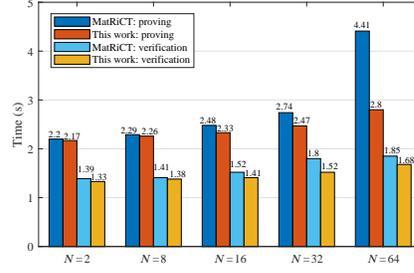


Fig. 5: Time cost of ring signatures.

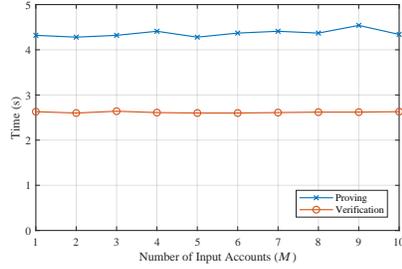


Fig. 6: Time cost of balance proofs with various inputs  $M$  when  $S = 1$ .

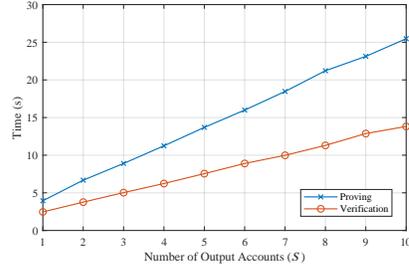


Fig. 7: Time cost of balance proofs with various outputs  $S$  when  $M = 1$ .

proving time of the MatRiCT, as we do not involve  $c_i$ 's in binary proofs. Besides, since the commitment of  $c_i$ 's is derived from  $A_i$ 's and  $B_i$ 's, our approach also reduce the time of committing to corrector values. Furthermore, our approach reduces nearly 20% verification time of the MatRiCT. The main reason is verifying the inner-product relation (step 35 of Protocol 2) is much more efficient than the balance relation with corrector values. The efficiency of binary verification is also improved when removing the corrector values.

The performances of ring signatures are depicted in Figure 5. Our unbalanced linear sum approach can reduce nearly 35% time of the one-out-of-many approach when  $N = 64$ . This is mainly contributed by avoiding the binary proof parts in our approach. When  $N$  is small, the binary proof/verification cost is only a small portion of the whole cost and thus the improvement is less significant. Besides, one interesting result is that the verification time does not increase much when  $N = 64$ . It is because we set  $\beta = 4$  and  $k = 3$  in this case, while in other cases  $\beta = N$  and  $k = 1$ . Though the verification time is greatly reduced under these settings, the proof size increases accordingly. Thus, for other cases, we keep  $\beta = N$  and  $k = 1$  as in [14]. Nevertheless, our approaches outperform MatRiCT in all settings.

Additionally, we show the proving and verification time of a balance proof for various inputs ( $M$ ) and outputs ( $S$ ) in Figure 6 and Figure 7 respectively. As a prover does not need to verify input accounts (input accounts have been

verifier in previous transactions as output accounts), there is almost no change in proving/verification time (similar as the result of proof size in Figure 1). Furthermore, the proving and verification time scales linearly with  $S$  since the prover needs to generate proofs for output accounts and the verifier needs to check these proofs accordingly. As stated in [14], “the most common cases for the number of input/output accounts are  $(M, S) = (1, 2)$  and  $(M, S) = (2, 2)$ ”, the time cost of our approaches are acceptable in most scenarios.

## 8 Extensions

We show how to apply our approaches in RingCT protocols and some extensions with other techniques.

**RingCT protocol.** In a RingCT protocol, a spender needs to prove a transaction is valid and hides the identity of input accounts at the same time. Additionally, the verifier should also check the input accounts (based on serial numbers) to avoid double spending. The former one can be achieved by adding hiding accounts into inputs. Considering  $NM$  inputs  $(\text{CN}_{in}^{(j)})_{j=0}^{N-1} = (A_i^{(j)})_{i=0, j=0}^{M-1, N-1}$ , which have  $M$  spender’s accounts,  $\text{CN}_{in}^{(l)}$  (the spender owns the amount values and coin keys  $(\mathbf{a}_i^{(l)}, \mathbf{r}_{a,i}^{(l)})_{i=0}^{M-1}$ ), and  $(N-1)M$  hiding accounts,  $\text{CN}_{in}^{(j)}$  where  $j \neq l$ . To transfer funds to  $S$  output accounts, the spender needs to send an additional commitment  $\text{Com}(\mathbf{c}; \mathbf{r}'_c)$  and compute public keys  $P_j$ ’s for each  $j \in [0, N)$ :

$$P_j = \sum_{i=0}^{S-1} B_i - \sum_{i=0}^{M-1} A_i^{(j)} - \text{Com}(\mathbf{c}; \mathbf{r}'_c). \quad (19)$$

Obviously,  $P_l$  is a commitment to zero with the private key (randomness)  $\mathbf{r} = \sum_{i=0}^{S-1} \mathbf{r}_{b,i} - \sum_{i=0}^{M-1} \mathbf{r}_{a,i} - \mathbf{r}'_c$ . Thus, the spender can further show  $P_l = \sum_{j=0}^{N-1} \delta_{l,j} P_j$  is a commitment to zero as in our ring signature scheme, which proves the amount balance and hides the identity at the same time.

To avoid double spending, we extend our ring signature to provide linkability by checking the serial number of each input account to ensure it is not included in previous transactions. Considering a new commitment key  $\mathbf{H}$ , a serial number is a commitment to zero under  $\mathbf{H}$  with the coin key as randomness, i.e.,  $S_i = \mathbf{H} \cdot \mathbf{r}_{a,i}$ . At step 14 of Protocol 3, the prover also needs to compute  $F_j^{(i)} = \mathbf{H} \cdot \boldsymbol{\rho}_j^{(i)}$  for all  $i \in [0, M)$ . Upon receiving the challenge  $x$ , the prover generates responses  $\mathbf{z}_r^{(i)} = x^k \mathbf{r}_{a,i} - \sum_{j=0}^{k-1} x^j \boldsymbol{\rho}_j^{(i)}$  at step 21. In the verification, the verifier should check 1) the serial numbers are distinct and not included in previous transactions to avoid double spending, and 2) the following equation holds to ensure serial numbers are correct:

$$x^k S_i - \sum_{j=0}^{k-1} x^j F_j^{(i)} = \mathbf{H} \cdot \mathbf{z}_r^{(i)}, \quad \forall i \in [0, M). \quad (20)$$

**Compatible with other techniques.** As we improve the underlying ZKPs of a RingCT protocol, our approaches preserve all distinguishing features of

MatRiCT, such as being compatible with efficient rejection sampling and extractable commitment techniques. The former one can be adopted in our unbalanced linear sum proof to improve the acceptance probability of rejection sampling. For a secret bit  $b \in \{0, 1\}$  and a challenge  $x \in [-p, p]$ , the prover can sample the masking value from a uniform distribution,  $a \leftarrow [-\mathcal{B}_a, \mathcal{B}_a]$  when  $b = 1$  or  $a \leftarrow [-(\mathcal{B}_a - p), \mathcal{B}_a - p]$  when  $b = 0$ . Thus,  $a$  will never be rejected when  $b = 0$ . When dealing with a binary secret with a fixed Hamming weight, this approach can improve the efficiency and avoid leaking side-channel information at the same time. The latter technique allows one to design an auditable RingCT protocol by placing a “mini trapdoor” in HMC. Setting  $\mathbf{G}_r = [\mathbf{A}, \mathbf{t}^\top]^\top$  as an LWE matrix where  $\mathbf{t} = \mathbf{A}^\top \mathbf{s} + \mathbf{e}$  for some secret  $\mathbf{s}$  (i.e., secret key for auditing) and error  $\mathbf{e}$ , an extractor can extract a message from a commitment  $C = \mathbf{G}_r \mathbf{r} + \mathbf{G}_m \mathbf{m}$  by computing  $\langle (\mathbf{s}, -1), C \rangle = -\langle \mathbf{e}, \mathbf{r} \rangle + \langle (\mathbf{s}, -1)^\top \mathbf{G}_m, \mathbf{m} \rangle$ . Based on the fact that the norm of  $\langle (\mathbf{s}, -1), C \rangle - \langle (\mathbf{s}, -1)^\top \mathbf{G}_m, \mathbf{m} \rangle$  is small, the extractor enumerates all possible values to recover  $\mathbf{m}$ .

Besides MatRiCT, other techniques to optimize the underlying cyclotomic rings [16] can also be applied in our approaches. Specifically, a new CRT-packing technique is proposed in power-of-2 cyclotomic rings to reduce the modulus with binary CRT slots (and reduce the commitment size accordingly). Furthermore, [16] optimizes challenges in cyclotomic rings to reduce their Hamming weights. As both techniques are “*general and of independent interest for lattice-based proof systems*” [16], our approaches can regard them as optimized settings to further improve efficiency. Besides, since corrector values are avoided in our solution, our balance proof can directly use these settings without mapping under Galois automorphisms for corrector values.

## 9 Discussion

**Applications in discrete logarithm settings.** Since our techniques do not rely on lattice settings, the results are believed to be of independent interest for RingCT protocols in a generic setting. The unbalanced linear sum proof can be applied in discrete logarithm settings directly to improve the performance of ring signatures by removing the binary proof part. Note that under the discrete logarithm assumption,  $b_i$ ’s do not necessarily have to be short as the constraint of “short  $b_i$ ’s” is only used to ensure the hiding and binding properties of HMC. Thus, steps 24 and 25 in Protocol 3 can be avoided accordingly (in fact, all norm checks can be avoided). However, the improvement of our unbalanced linear sum proof may be less significant as the binary proof does not require a larger parameter set under discrete logarithm assumptions. For the linear equation satisfiability, it is compatible with bit-based commitments with Equation (13) (commit to the bits of the witness instead of its value directly). Note that bit-based commitments bring some advantages in existing RingCT protocols: a binary proof implies a range proof relation directly. With our linear equation satisfiability, we can build the balance and range relations in a different way. Furthermore, the linear equation satisfiability has a wider application in any-

mous DeFi applications (decentralized finance smart contracts on Ethereum). By settings  $\omega_i$ 's as the exchange rates of different pools, we can enable confidential multi-pool transactions (inputs and outputs are from distinct pools) for today's anonymous DeFi such as Zether [9].

**General-purpose lattice-based proof systems.** Since we do not exploit any special property of the commitment scheme other than the standard hiding and binding properties, other approaches with intriguing properties in general-purpose lattice-based proof systems [2, 8] may be applied in our scenarios. In standard SIS commitment schemes, the witness is a  $(v \times l)$ -size matrix,  $S \in \mathbb{Z}_q^{v \times l}$ . With a  $(r \times v)$ -size matrix  $A \in \mathbb{Z}_q^{r \times v}$ , the commitment works as  $\text{Com}(S) = A \cdot S = T \in \mathbb{Z}_q^{r \times l}$ . Based on an  $(l \times n)$ -size challenge  $C \in \{0, 1\}^{l \times n}$ , the prover encodes  $S$  as  $Z = S \cdot C + Y$  with  $Y \in D_\sigma^{v \times n}$ .

First, an  $O(\sqrt{N})$ -size commitment scheme is proposed in [2] by encoding  $N$ -many secrets into  $S$  where  $v = l = O(\sqrt{N})$ . Unfortunately, when adopting this approach, the  $\langle \mathbf{f}, \mathbf{2}^k \rangle$  in Equation (15) cannot be calculated directly as  $Z$  will “batch” some  $f_i$ 's when computing  $S \cdot C$ . For instance, consider the first element in  $Z$ ,  $z_{0,0} = \sum_{i=0}^{l-1} s_{0,i} \cdot c_{i,0} + y_{0,0}$ . As  $f_0 = s_{0,0} \cdot c_{0,0} + y_{0,0}$ , we have  $2^0 \cdot z_{0,0} = 2^0 \cdot f_0 + 2^0 \cdot (\sum_{i=1}^{l-1} s_{0,i} \cdot c_{i,0}) = 2^0 \cdot f_0 + 2^0 \cdot e_0$ . Therefore, it is important to allow the verifier to cancel out  $\sum_{i=0}^{k-1} 2^i \cdot e_i$  without leaking any information when computing  $\langle \mathbf{f}, \mathbf{2}^k \rangle$ . The same issue occurs in ring signatures when computing  $\sum_{i=0}^{\beta-1} f_{j,i}$  in Equation (16) and  $\prod_{j=0}^{k-1} f_{l_j, i_j}$  in Equation (17). The latter one is a much thornier problem when using  $z_{i,j}$ 's to compute  $\prod_{j=0}^{k-1} f_{j, i_j}$ . Second, levelled commitments and Bulletproofs folding are proposed in [8]. The proof size can be reduced to  $O(N^{\frac{1}{d+1}})$  with  $d$ -levelled commitments or  $O(\log^2(N))$  with Bulletproofs folding. Though the result is promising, we find it is hard to be applied in our approaches due to the same reasons above. Besides, the sizes of the extracted solutions (denoted by “slack” in [8]) also increase. Generally speaking, we cannot directly apply these approaches if the response batches  $f_i$ 's.

**Open problems.** Our ring signature approach avoids most of the binary proof in existing approaches based on the fact that a one-out-of-many relation is not a *necessary* condition for ring signatures. An interesting question is finding the *sufficient and necessary* condition for ring signatures. We may further avoid unnecessary parts of our linear sum proof to improve the efficiency of ring signatures. Another interesting problem is to remove unnecessary parts in range proofs or balance proofs. For instance, it is sufficient to prove the balance based on Equation (10) even when  $\mathbf{a}_i$ 's and  $\mathbf{b}_i$ 's are not binary vectors. However, this requires additional proofs to show  $\langle \mathbf{a}_i, \mathbf{2}^k \rangle \geq 0$  and  $\langle \mathbf{b}_i, \mathbf{2}^k \rangle \geq 0$ , which may not be efficient. Furthermore, the linear sum relation yields a “many-out-of-many” relation [13] which can reduce the anonymity set in RingCT. Unlike [13] which generates *many* public key index from a *single* secret  $l$  by permutations and a linear mapping, the linear sum relation directly maps  $b_i$ 's to  $P_i$ 's which may be more efficient. Thus, the logarithmic-size linear sum proof seems to be a promising solution. Finally, supporting other commitment schemes in general-purpose lattice-based proof systems [2, 8] is also promising.

## 10 Acknowledgment

We gratefully acknowledge Dr. Xingye LU from the University of Hong Kong for the helpful technical discussions about lattice-based cryptography as well as Dr. Zuoxia Yu from University of Wollongong Dr. Aoning HU from the Southeast University for the discussion about ring signatures. We would also like to thank to the reviewers of Oakland'20 and Oakland'21 for their valuable comments. This research is partially supported by HK RGC GRF PolyU 15216721/Q86A and HK PolyU Start-Up ZVUE.

## References

1. Albrecht, M.R., Player, R., Scott, S.: On the Concrete Hardness of Learning With Errors. In: *Journal of Mathematical Cryptology* (2015)
2. Baum, C., Bootle, J., Cerulli, A., Del Pino, R., Groth, J., Lyubashevsky, V.: Sub-linear Lattice-based Zero-knowledge Arguments for Arithmetic Circuits. In: *Proc. of the Annual International Cryptology Conference (CRYPTO)*. Springer (2018)
3. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More Efficient Commitments from Structured Lattice Assumptions. In: *Proc. of the International Conference on Security and Cryptography for Networks (SCN)*. Springer (2018)
4. Baum, C., Lin, H., Oechsner, S.: Towards Practical Lattice-Based One-Time Linkable Ring Signatures. In: *Proc. of the International Conference on Information and Communications Security (ICICS)*. Springer (2018)
5. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., Virza, M.: SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. In: *Proc. of the Annual International Cryptology Conference (CRYPTO)*. Springer (2013)
6. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J., Petit, C.: Short Accountable Ring Signatures Based on DDH. In: *Proc. of the European Symposium on Research in Computer Security (ESORICS)*. Springer (2015)
7. Bootle, J., Cerulli, A., Chaidos, P., Groth, J., Petit, C.: Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. In: *Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer (2016)
8. Bootle, J., Lyubashevsky, V., Nguyen, N.K., Seiler, G.: A Non-PCP Approach to Succinct Quantum-safe Zero-knowledge. In: *Proc. of the Annual International Cryptology Conference (CRYPTO)*. Springer (2020)
9. Bünz, B., Agrawal, S., Zamani, M., Boneh, D.: Zether: Towards Privacy in a Smart Contract World. In: *Proc. of the International Conference on Financial Cryptography and Data Security (FC)*. Springer (2020)
10. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: Short Proofs for Confidential Transactions and More. In: *Proc. of the IEEE Symposium on Security and Privacy (Oakland)*. IEEE (2018)
11. Dagdelen, Ö., Fischlin, M., Gagliardoni, T.: The Fiat-Shamir Transformation in a Quantum World. In: *Proc. of the Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer (2013)
12. Del Pino, R., Lyubashevsky, V., Seiler, G.: Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability. In: *Proc. of the ACM Conference on Computer & Communications Security (CCS)*. ACM (2018)

13. Diamond, B.E.: “Many-out-of-Many” Proofs with Applications to Anonymous Zether. In: Proc. of the IEEE Symposium on Security and Privacy (Oakland). IEEE (2020)
14. Esgin, M.F., Steinfeld, R., Liu, J.K., Liu, D.: Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications. In: Proc. of the Annual International Cryptology Conference (CRYPTO). Springer (2019)
15. Esgin, M.F., Steinfeld, R., Sakzad, A., Liu, J.K., Liu, D.: Short Lattice-Based One-Out-of-Many Proofs and Applications to Ring Signatures. In: Proc. of the International Conference on Applied Cryptography and Network Security (ACNS). Springer (2019)
16. Esgin, M.F., Steinfeld, R., Zhao, R.K.: MatRiCT+: More Efficient Post-Quantum Private Blockchain Payments. In: IACR Cryptology ePrint Archive (2021)
17. Esgin, M.F., Zhao, R.K., Steinfeld, R., Liu, J.K., Liu, D.: MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. In: Proc. of the ACM Conference on Computer & Communications Security (CCS). ACM (2019)
18. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive Arguments of Knowledge. In: IACR Cryptology ePrint Archive (2019)
19. Gao, S.: RingCT Implementation. <https://github.com/Anonymous-000/RingCT> (2021)
20. Groth, J.: On the Size of Pairing-based Non-Interactive Arguments. In: Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer (2016)
21. Groth, J., Kohlweiss, M.: One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin. In: Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer (2015)
22. Kiltz, E., Lyubashevsky, V., Schaffner, C.: A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. In: Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer (2018)
23. Langlois, A., Stehlé, D.: Worst-Case to Average-Case Reductions for Module Lattices. In: Designs, Codes and Cryptography. Springer
24. Li, S., Jovanovic, P., ChristianMct: LAGO. <https://github.com/dedis/lago> (2021)
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: Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer (2016)
26. Lu, X., Au, M.H., Zhang, Z.: Raptor: A Practical Lattice-Based (Linkable) Ring Signature. In: Proc. of the International Conference on Applied Cryptography and Network Security (ACNS). Springer (2019)
27. Lyubashevsky, V.: Lattice Signatures Without Trapdoors. In: Proc. of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer (2012)
28. Noether, S.: Ring Signature Confidential Transactions for Monero. In: IACR Cryptology ePrint Archive (2015)
29. Noether, S., Mackenzie, A., et al.: Ring Confidential Transactions. In: Ledger (2016)

30. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly Practical Verifiable Computation. In: Proc. of the IEEE Symposium on Security and Privacy (Oakland). IEEE (2013)
31. Poelstra, A., Back, A., Friedenbach, M., Maxwell, G., Wuille, P.: Confidential Assets. In: Proc. of the International Conference on Financial Cryptography and Data Security (FC). Springer (2018)
32. Project, M.: Monero. <https://www.getmonero.org/> (2020)
33. Rivest, R.L., Shamir, A., Tauman, Y.: How to Leak a Secret. In: Proc. of the Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer (2001)
34. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized Anonymous Payments from Bitcoin. In: Proc. of the IEEE Symposium on Security and Privacy (Oakland). IEEE (2014)
35. Sun, S.F., Au, M.H., Liu, J.K., Yuen, T.H.: RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. In: Proc. of the European Symposium on Research in Computer Security (ESORICS). Springer (2017)
36. Torres, W.A.A., Steinfeld, R., Sakzad, A., Liu, J.K., Kuchta, V., Bhattacharjee, N., Au, M.H., Cheng, J.: Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). In: Proc. of the Australasian Conference on Information Security and Privacy (ACISP). Springer (2018)
37. 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. In: IACR Cryptology ePrint Archive (2017)
38. Yuen, T.H., Sun, S.f., Liu, J.K., Au, M.H., Esgin, M.F., Zhang, Q., Gu, D.: RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security. In: Cryptology ePrint Archive (2019)

## A Additional Lemmas

**Lemma 6.** (*Lemma 8 in [14]*) For any  $f, g \in R = \mathbb{Z}[X]/(X^d + 1)$ , we have the following relations:

- $\|f\| \leq \sqrt{d} \cdot \|f\|_\infty$ ,
- $\|f\| \leq \|f\|_1 \leq \sqrt{d} \cdot \|f\|$ ,
- $\|f \cdot g\| \leq \sqrt{d} \cdot \|f\| \cdot \|g\|$ ,
- $\|f \cdot g\|_\infty \leq \|f\| \cdot \|g\|$ ,
- $\|f \cdot g\|_\infty \leq \|f\|_1 \cdot \|g\|_\infty$ ,
- $\|\prod_{i=1}^n f_i\|_\infty \leq (\prod_{i=1}^{n-1} \|f_i\|_1) \cdot \|f_n\|_\infty$ .

**Lemma 7.** (*Theorem 4.4 in [27]*)

- For any  $k > 0$ ,  $\Pr[|z| > k\sigma; z \leftarrow D_\sigma] \leq 2e^{-k^2/2}$ .
- For any  $k > 1$ ,  $\Pr[\|z\| > k\sigma\sqrt{s}; z \leftarrow D_\sigma^s] < k^s e^{s(1-k^2)/2}$ .

**Lemma 8.** (*Theorem 4.6 in [27]*) Let  $h$  be a probability distribution over  $V \in \mathbb{Z}^s$  where  $s \geq 1$  and the norm of all elements is less than  $T$ . Let  $\mathbf{c} \leftarrow h$  and  $\phi > 0$ . Considering an algorithm that samples  $\mathbf{y} \leftarrow D_\sigma^s$  and outputs  $\text{Rej}(\mathbf{z}, \mathbf{c}, \phi, T)$  for  $\mathbf{z} = \mathbf{y} + \mathbf{c}$ . The probability that the algorithm outputs 1 is within  $2^{-100}$  of  $1/\mu(\phi)$  where  $\mu(\phi) = e^{12/\phi + 1/(2\phi^2)}$ . When the output is 1, the statistical distance between the distribution of  $\mathbf{z}$  and  $D_\sigma^s$  is at most  $2^{-100}$ .

**Lemma 9.** (*Lemma 6 in [14]*) For  $f, g \in R$  and  $k \in \mathbb{Z}^*$ , if  $f \cdot g^k = 0$  in  $R_q$ , then  $f \cdot g = 0$  in  $R_q$ .

**Lemma 10.** Considering independent vectors  $\mathbf{y}_1, \dots, \mathbf{y}_s$  with distributions  $D_{\sigma_1}^d, \dots, D_{\sigma_s}^d$  for  $d \geq 1$ . If  $\sigma_i \geq \tau(\mathbb{Z}^d)/\sqrt{\pi}$  for all  $i \in [1, s]$  where  $\tau(\mathbb{Z}^d)$  is a smoothing parameter of  $\mathbb{Z}^d$ , the distribution of  $\sum_{i=1}^s \mathbf{y}_i$  is statistically close to  $D_{\sqrt{\sum_{i=1}^s \sigma_i^2}}^d$ .

In particular, we have the distribution of  $\sum_{i=1}^s \mathbf{y}_i$  is statistically close to  $D_{\sigma\sqrt{s}}^d$  if  $D_{\sigma_i}^d = D_\sigma^d$  (**Lemma 9 in [14]**) and the distribution of  $\sum_{i=1}^s \mathbf{y}_i$  is statistically close to  $D_{\sigma\sqrt{\sum_{i=1}^s 2^i}}^d$  if  $D_{\sigma_i}^d = D_{\sigma\sqrt{2^i}}^d$  for all  $i \in [1, s]$ .

## B Proof of Theorem 1

*Proof. Completeness:* Based on Lemma 8, the prover responds with probability  $1/(\mu(\phi_1)\mu(\phi_2)\mu(\phi_3))$ . As there are at most  $kN$ -many 1's in  $\mathbf{b}$  and  $\text{HW}(x) = w$ , we have at most  $wkN$  non-zero elements in  $x\mathbf{b}$ . Since  $\|x\|_\infty = p$ , we have,

$$\|x\mathbf{b}\| \leq p\sqrt{wkN} = T_1. \quad (21)$$

Furthermore, we have  $\|\mathbf{c}\|_\infty \leq \max(-\sum_{\omega_i < 0} \omega_i, \sum_{\omega_i > 0} \omega_i)$  based on  $c_j = \sum_{i=0}^{N-1} \omega_i b_{i,j} \in [\sum_{\omega_i < 0} \omega_i, \sum_{\omega_i > 0} \omega_i]$ . Since there are at most  $k$  non-zero elements in  $\mathbf{c}$  and  $HW(x) = w$ ,  $x\mathbf{c}$  has at most  $wk$  non-zero elements. Thus,

$$\|x\mathbf{c}\| \leq \max(-\sum_{\omega_i < 0} \omega_i, \sum_{\omega_i > 0} \omega_i) \cdot p\sqrt{wk} = T_2. \quad (22)$$

Let  $\boldsymbol{\omega} = (\omega_0, \dots, \omega_{N-1})$ . Based on Lemma 6, we have

$$\begin{aligned} \|\mathbf{r}_c\| &= \left\| \sum_{i=0}^{N-1} \omega_i \mathbf{r}_{b,i} \right\| \leq \sum_{i=0}^{N-1} (|\omega_i| \cdot \|\mathbf{r}_{b,i}\|) \\ &\leq \sqrt{md} \cdot \|\mathbf{r}_{b,i}\|_\infty \cdot \|\boldsymbol{\omega}\|_1 \leq \mathcal{B}\sqrt{md}\|\boldsymbol{\omega}\|_1, \end{aligned} \quad (23)$$

and thus,

$$\begin{aligned} &\|x(\mathbf{r}_c, \mathbf{r}_b, \mathbf{r}_{b,0}, \dots, \mathbf{r}_{b,N-1})\| \\ &= (\|x\mathbf{r}_c\|^2 + \|x(\mathbf{r}_b, \mathbf{r}_{b,0}, \dots, \mathbf{r}_{b,N-1})\|^2)^{1/2} \\ &\leq \mathcal{B}wp\sqrt{md(\|\boldsymbol{\omega}\|_1^2 + N + 1)} = T_3. \end{aligned} \quad (24)$$

Therefore, based on Lemma 8, the distributions of  $g_{i,j}$ 's,  $f_j$ 's, and  $\mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1}$  are statistically close to  $D_{\phi_1 T_1}^d, D_{\phi_2 T_2}^d$ , and  $D_{\phi_3 T_3}^{md}$ , respectively. Except with negligible probability, we have the following relations based on Lemma 7:

$$\begin{aligned} \|g_{i,j}\| &\leq 2(\phi_1 T_1)\sqrt{d}, \quad \forall i \in [0, N), j \in [0, k), \\ \|f_j\| &\leq 2(\phi_2 T_2)\sqrt{d}, \quad \forall j \in [1, k), \\ \|\mathbf{z}\|, \|\mathbf{z}_g\|, (\|\mathbf{z}_{b,i}\|)_{i=0}^{N-1} &\leq 2(\phi_3 T_3)\sqrt{md}, \end{aligned} \quad (25)$$

which satisfy steps 38, 39, and 41 of verification.

Finally, we compute the bound of  $\|f_0\|$ . According to Lemma 10, the distribution of  $\sum_{j=1}^{k-1} 2^j f_j$  is statistically close to  $D_{\phi_2 T_2 \sqrt{\sum_{i=1}^{k-1} 2^i}}^d$ . Hence, we have

$$\|f_0\| = \left\| -\sum_{j=1}^{k-1} 2^j f_j \right\| \leq 2(\phi_2 T_2) \left( \sum_{i=1}^{k-1} 2^i \right)^{\frac{1}{2}} \sqrt{d} \leq 2\phi_2 T_2 \sqrt{2^k d},$$

which satisfies step 40 of verification.

**3-special soundness:** Given 3 distinct challenges,  $(x, x', x'')$ , we have 3 accepted responses  $(\mathbf{f}_1, \mathbf{g}, \mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1})$ ,  $(\mathbf{f}'_1, \mathbf{g}', \mathbf{z}', \mathbf{z}'_g, (\mathbf{z}'_{b,i})_{i=0}^{N-1})$ , and  $(\mathbf{f}''_1, \mathbf{g}'', \mathbf{z}'', \mathbf{z}''_g, (\mathbf{z}''_{b,i})_{i=0}^{N-1})$  with the same inputs and commitments  $(B_i)_{i=0}^{N-1}, D, E, F, (G_i)_{i=0}^{N-1}$ . Set  $C = \sum_{i=0}^{N-1} \omega_i B_i$ . For each transcript, compute  $f_0 = -\sum_{j=1}^{k-1} 2^j \cdot f_j$  and rebuild  $\mathbf{f} = (f_0, \dots, f_{k-1})$ . Obviously, we have  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$  (so do  $\mathbf{f}'$  and  $\mathbf{f}''$ ). Taking  $(\mathbf{f}, \mathbf{z})$ ,  $(\mathbf{f}', \mathbf{z}')$ , and  $(\mathbf{f}'', \mathbf{z}'')$ ,

we have

$$xC + D = \text{Com}_{ck}(\mathbf{f}; \mathbf{z}), \quad (26)$$

$$x'C + D = \text{Com}_{ck}(\mathbf{f}'; \mathbf{z}'), \quad (27)$$

$$x''C + D = \text{Com}_{ck}(\mathbf{f}''; \mathbf{z}''). \quad (28)$$

Subtracting Equation (27) from Equation (26), we get

$$(x - x')C = \text{Com}_{ck}(\mathbf{f} - \mathbf{f}'; \mathbf{z} - \mathbf{z}') := \text{Com}_{ck}(\widehat{\mathbf{c}}; \widehat{\mathbf{r}}_c). \quad (29)$$

Considering  $\|\widehat{\mathbf{r}}_c\| = \|\mathbf{z} - \mathbf{z}'\| \leq 4\phi_3 T_3 \sqrt{md} = 4\phi_3 md \mathcal{Bwp}(\|\boldsymbol{\omega}\|_1^2 + N + 1)^{1/2} = \gamma_{LE}$  and setting  $y = x - x'$  as a relaxation factor, we extract a valid opening  $(\widehat{\mathbf{c}}; \widehat{\mathbf{r}}_c)$  to  $yC$  and prove the claimed bound for  $\mathcal{R}'_{LE}$ .

Taking Equation (29) and (26), we have

$$\begin{aligned} yD &= y(xC + D) - xyC = \text{Com}_{ck}(y\mathbf{f} - x\widehat{\mathbf{c}}; y\mathbf{z} - x\widehat{\mathbf{r}}_c) \\ &= \text{Com}_{ck}(x\mathbf{f}' - x'\mathbf{f}; x\mathbf{z}' - x'\mathbf{z}) := \text{Com}_{ck}(\widehat{\mathbf{d}}; \widehat{\mathbf{r}}_d). \end{aligned} \quad (30)$$

Obviously, based on the definition of  $\widehat{\mathbf{c}}$  and  $\widehat{\mathbf{d}}$ , we have  $y\mathbf{f} = x\widehat{\mathbf{c}} + \widehat{\mathbf{d}}$ .

As we conduct step 35 on  $R$  instead of  $R_q$ , we have  $\langle \mathbf{f}, \mathbf{2}^k \rangle = 0$ , and thus  $x\langle \widehat{\mathbf{c}}, \mathbf{2}^k \rangle + \langle \widehat{\mathbf{d}}, \mathbf{2}^k \rangle = 0$ . Based on the  $\gamma_{LE}$ -binding property of the commitment scheme, the PPT prover cannot extract a new valid opening of  $yC$  and  $yD$  with non-negligible probability. Thus, we also have  $x'\langle \widehat{\mathbf{c}}, \mathbf{2}^k \rangle + \langle \widehat{\mathbf{d}}, \mathbf{2}^k \rangle = 0$ , which implies  $\langle \widehat{\mathbf{c}}, \mathbf{2}^k \rangle = 0$  for distinct challenges. Considering the definition of  $C$ , we have

$$C = \sum_{i=0}^{N-1} \omega_i B_i = \text{Com}_{ck}\left(\sum_{i=0}^{N-1} \omega_i \mathbf{b}_i; \sum_{i=0}^{N-1} \omega_i \mathbf{r}_{b,i}\right), \quad (31)$$

and thus

$$\begin{aligned} y\left\langle \sum_{i=0}^{N-1} \omega_i \mathbf{b}_i, \mathbf{2}^k \right\rangle &= \langle \widehat{\mathbf{c}}, \mathbf{2}^k \rangle = 0 \\ \implies \sum_{i=0}^{N-1} \left( \omega_i \cdot \langle \mathbf{2}^k, \mathbf{b}_i \rangle \right) &= F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0, \end{aligned} \quad (32)$$

which proves the  $F'(\mathbf{b}_0, \dots, \mathbf{b}_{N-1}) = 0$  relation in  $\mathcal{R}'_{LE}$ .

Furthermore, we can use a similar approach to derive the opening  $((\widehat{\mathbf{b}}, \widehat{\mathbf{e}}); \widehat{\mathbf{r}}_b)$  to  $yE$  and  $((\widehat{\mathbf{t}}, \widehat{\mathbf{s}}); \widehat{\mathbf{r}}_t)$  to  $yF$  such that  $y\mathbf{g} = x\widehat{\mathbf{b}} + \widehat{\mathbf{t}}$  and  $y\mathbf{h} = x\widehat{\mathbf{e}} + \widehat{\mathbf{s}}$ . Thus, for each element of  $\mathbf{g}$  and  $\mathbf{h}$ , we have the following relations for all  $i \in [0, N)$  and  $j \in [0, k)$ :

$$\begin{aligned} yg_{i,j} &= x\widehat{b}_{i,j} + \widehat{t}_{i,j}, \\ yh_{i,j} &= y(g_{i,j}(x - g_{i,j})) = x\widehat{e}_{i,j} + \widehat{s}_{i,j}. \end{aligned} \quad (33)$$

Based on the  $\gamma_{LE}$ -binding property of the commitment scheme, the PPT prover cannot extract a new valid opening of  $yE$  and  $yF$  with non-negligible probability. Thus, the responses to  $x''$  will have the same form in Equation (33), which indicates Equation (33) holds for  $x, x', x''$ .

Based on Equation (33), we have the following equation:

$$\begin{aligned} y(x\widehat{e}_{i,j} + \widehat{s}_{i,j}) &= y(yg_{i,j}(x - g_{i,j})) \\ &= yg_{i,j}(xy - yg_{i,j}) = (x\widehat{b}_{i,j} + \widehat{t}_{i,j})(xy - x\widehat{b}_{i,j} - \widehat{t}_{i,j}) \\ &= x^2(\widehat{b}_{i,j}(y - \widehat{b}_{i,j})) + x(\widehat{t}_{i,j}(y - 2\widehat{b}_{i,j})) - \widehat{t}_{i,j}^2, \end{aligned} \quad (34)$$

and thus

$$\begin{aligned} x^2(\widehat{b}_{i,j}(y - \widehat{b}_{i,j})) + x(\widehat{t}_{i,j}(y - 2\widehat{b}_{i,j}) - y\widehat{e}_{i,j}) \\ + (-\widehat{t}_{i,j}^2 - y\widehat{s}_{i,j}) = 0, \end{aligned} \quad (35)$$

Since Equation (35) holds for  $x, x'$ , and  $x''$ , we have the following system:

$$\begin{pmatrix} 1 & x & x^2 \\ 1 & x' & x'^2 \\ 1 & x'' & x''^2 \end{pmatrix} \cdot \begin{pmatrix} -\widehat{t}_{i,j}^2 - y\widehat{s}_{i,j} \\ \widehat{t}_{i,j}(y - 2\widehat{b}_{i,j}) - y\widehat{e}_{i,j} \\ \widehat{b}_{i,j}(y - \widehat{b}_{i,j}) \end{pmatrix} = \mathbf{0}. \quad (36)$$

As all operations are conducted on a field  $R_q$ , the Vandermonde matrix on the left is invertible for distinct challenges. We have  $\widehat{b}_{i,j}(y - \widehat{b}_{i,j}) = 0$ , which implies  $\widehat{b}_{i,j} = 0$  or  $\widehat{b}_{i,j} = y$ , i.e.,  $\widehat{b}_{i,j} = yb_{i,j}$  for  $b_{i,j} \in \{0, 1\}$ . Thus, all  $\widehat{\mathbf{b}}_i$ 's are binary vectors.

Finally, we verify the extracted values are valid openings. Based on the last verification step, for all  $i \in [0, N)$ , we can also derive the opening  $(\widehat{\mathbf{b}}_i; \widehat{\mathbf{r}}_{b,i})$  to  $yB_i$  and  $(\widetilde{\mathbf{t}}_i; \widetilde{\mathbf{r}}_{t,i})$  to  $yG_i$  such that  $y\mathbf{g}_i = x\widetilde{\mathbf{b}}_i + \widetilde{\mathbf{t}}_i$  (here we use  $\widetilde{\mathbf{b}}_i$  instead of  $\widehat{\mathbf{b}}_i$  to distinguish between the elements of  $\widetilde{\mathbf{b}}_i$  and  $\widehat{\mathbf{b}}_i$ ). Taking the first equation of (33), for each element of  $\mathbf{g}_i$ , we have the following relation for all  $j \in [0, k)$ :

$$yg_{i,j} = x\widetilde{b}_{i,j} + \widetilde{t}_{i,j} = x\widehat{b}_{i,j} + \widehat{t}_{i,j}, \quad (37)$$

and thus

$$x(\widetilde{b}_{i,j} - \widehat{b}_{i,j}) + (\widetilde{t}_{i,j} - \widehat{t}_{i,j}) = 0. \quad (38)$$

As Equation (38) holds for all distinct challenges based on the  $\gamma_{LE}$ -binding property of the commitment scheme, we have  $\widetilde{b}_{i,j} = \widehat{b}_{i,j}$  and  $\widetilde{t}_{i,j} = \widehat{t}_{i,j}$ , which implies for all  $i \in [0, N)$ ,  $\widehat{\mathbf{b}}_i$  and  $\widehat{\mathbf{t}}_{i,j}$  are exact openings to  $yB_i$  and  $yG_i$  respectively.

**SHVZK:** Assume the protocol is not aborted. The simulator samples  $\mathbf{r}_b \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$ ,  $g_{i,j} \leftarrow D_{\phi_1 T_1}^d$  for all  $i \in [0, N)$  and  $j \in [0, k)$ ,  $f_j \leftarrow D_{\phi_2 T_2}^d$  for all  $j \in [0, k)$ ,  $\mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1} \leftarrow D_{\phi_3 T_3}^{md}$ , and sets  $C = \sum_{i=0}^{N-1} \omega_i B_i$ ,  $E = \text{Com}_{ck}(\mathbf{0}; \mathbf{r}_b)$ ,  $\mathbf{f}_1 = (f_1, \dots, f_{k-1})$ ,  $f_0 = -\sum_{j=1}^{k-1} 2^j f_j$ ,  $\mathbf{f} = (f_0, \dots, f_{k-1})$ ,

$\mathbf{g} = (g_{0,0}, \dots, g_{s-1,k-1})$ ,  $\mathbf{g}_i = (g_{i,0}, \dots, g_{i,k-1})$  for all  $i \in [0, N)$ . Then, given  $x$ , it computes  $\mathbf{h} = (g_{i,j}(x - g_{i,j}))_{i=0, j=0}^{N-1, k-1}$ ,  $D = \text{Com}_{ck}(\mathbf{f}; \mathbf{z}) - xC$ ,  $F = \text{Com}_{ck}(\mathbf{g}, \mathbf{h}; \mathbf{z}_g) - xE$ , and  $G_i = \text{Com}_{ck}(\mathbf{g}_i; \mathbf{z}_{b,i}) - xB_i$  for all  $i \in [0, N)$ . Obviously, the simulated transcript  $((D, E, F, (G_i)_{i=0}^{N-1}), x, (\mathbf{f}_1, \mathbf{g}, \mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1}))$  will be an accepted transcript.

Based on Lemma 7, the distributions of  $\mathbf{f}_1, \mathbf{g}, \mathbf{z}, \mathbf{z}_g, (\mathbf{z}_{b,i})_{i=0}^{N-1}$  are statistically close to the real distributions. The simulated distributions of  $D, F, (G_i)_{i=0}^{N-1}$  are the same as the real distributions. Finally, due to the hiding property of the commitment scheme, the distribution of simulated  $E$  is computationally indistinguishable from the real case based on the M-LWE assumption.

## C Proof of Theorem 2

*Proof. Completeness:* Based on Lemma 8, the prover responds with probability  $1/(\mu(\phi_1)\mu(\phi_2))$ . As there are at most  $k$ -many 1's in  $\delta$  and  $HW(x) = w$ , we have at most  $wk$ -many non-zero elements in  $x\delta$ . Since  $\|x\|_\infty = p$ , we have,

$$\|x\delta\| \leq p\sqrt{wk} = T_1. \quad (39)$$

Furthermore, based on Lemma 6, we have

$$\begin{aligned} \left\| x^k \mathbf{r} - \sum_{j=1}^{k-1} x^j \boldsymbol{\rho}_j \right\| &\leq \|x^k \mathbf{r}\| + \sum_{j=1}^{k-1} \|x^j \boldsymbol{\rho}_j\| \\ &\leq \sqrt{md} \left( \|x^k \mathbf{r}\|_\infty + \sum_{j=1}^{k-1} \|x^j \boldsymbol{\rho}_j\|_\infty \right) \\ &\leq \sqrt{md} \left( \|x\|_1^k \cdot \|\mathbf{r}\|_\infty + \sum_{j=1}^{k-1} \|x\|^j \cdot \|\boldsymbol{\rho}_j\|_\infty \right) \\ &\leq \sqrt{md} \left( (wp)^k \mathcal{B} + \mathcal{B} \sum_{j=1}^{k-1} (wp)^j \right) = \mathcal{B} \sqrt{md} \sum_{j=1}^k (wp)^j. \end{aligned} \quad (40)$$

Denote  $\mathbf{r}' = x^k \mathbf{r} - \sum_{j=1}^{k-1} x^j \boldsymbol{\rho}_j$ , we have

$$\begin{aligned} \|x\mathbf{r}_b, \mathbf{r}'\| &= (\|x\mathbf{r}_b\|^2 + \|\mathbf{r}'\|^2)^{1/2} \\ &\leq \mathcal{B} \sqrt{md} \left( w^2 p^2 + \left( \sum_{j=1}^k w^j p^j \right)^2 \right)^{1/2} \leq \mathcal{B} (wp)^k \sqrt{2md} = T_2. \end{aligned} \quad (41)$$

Considering each element of  $\mathbf{f}_1$ . Based on Lemma 10, the sum of discrete normal variables behaves as its continuous counterpart. Thus, for all  $j \in [0, k)$ , we have the distribution of  $\sum_{i=1}^{\beta-1} f_{j,i}$  is statistically close to  $D_{\phi_1 T_1 \sqrt{\beta-1}}^d$ . Therefore,

for all  $j \in [0, k)$  and  $i \in (0, \beta)$ , we have

$$\begin{aligned} \|f_{j,i}\| &\leq 2(\phi_1 T_1) \sqrt{d}, \\ \|f_{j,0}\| &\leq \left\| x - \sum_{i=1}^{\beta-1} f_{j,i} \right\| \leq \|x\| + \left\| \sum_{i=1}^{\beta-1} f_{j,i} \right\| \\ &\leq \sqrt{w} + 2(\phi_1 T_1) \sqrt{d(\beta-1)} \approx 2\phi_1 p \sqrt{kwd\beta}, \\ \|\mathbf{z}_b\|, \|\mathbf{z}_r\| &\leq 2(\phi_2 T_2) \sqrt{md}. \end{aligned} \quad (42)$$

**( $k+1$ )-special soundness:** Given  $(k+1)$  distinct challenges  $(x_s)_{s=0}^k$ , we have  $(k+1)$  accepted responses  $(\mathbf{f}_1^{(s)}, \mathbf{z}_b^{(s)})_{s=0}^k$  with the same commitments  $A, B, (E_j)_{j=0}^{k-1}$ . For each transcript, compute  $\mathbf{f}_{j,0}^{(s)} = x_s - \sum_{i=1}^{\beta-1} f_{i,j}^{(s)}$  for all  $j \in [0, k)$ , and rebuild  $\mathbf{f}^{(s)} = (f_{0,0}^{(s)}, \dots, f_{k-1,\beta-1}^{(s)})$ . Taking  $(\mathbf{f}^{(0)}, \mathbf{z}_b^{(0)})$  and  $(\mathbf{f}^{(1)}, \mathbf{z}_b^{(1)})$ , we have

$$x_0 B + A = \text{Com}_{ck}(\mathbf{f}^{(0)}, \mathbf{z}_b^{(0)}), \quad (43)$$

$$x_1 B + A = \text{Com}_{ck}(\mathbf{f}^{(1)}, \mathbf{z}_b^{(1)}). \quad (44)$$

Subtracting (44) from (43), we get  $(x_0 - x_1)B = \text{Com}_{ck}(\mathbf{f}^{(0)} - \mathbf{f}^{(1)}, \mathbf{z}_b^{(0)} - \mathbf{z}_b^{(1)})$ , which gives us an opening of  $yB$  with a relaxation factor  $y = (x_0 - x_1)$ :

$$yB = \text{Com}_{ck}(\mathbf{f}^{(0)} - \mathbf{f}^{(1)}, \mathbf{z}_b^{(0)} - \mathbf{z}_b^{(1)}) := \text{Com}_{ck}(\widehat{\mathbf{b}}, \widehat{\mathbf{r}}_b). \quad (45)$$

Subtracting  $x_0$  times of (45) from  $y$  times of (43), we have:

$$\begin{aligned} yA &= \text{Com}_{ck}(y\mathbf{f}^{(0)} - x_0\widehat{\mathbf{b}}; \quad y\mathbf{z}_b^{(0)} - x_0\widehat{\mathbf{r}}_b) \\ &= \text{Com}_{ck}(x_0\mathbf{f}^{(1)} - x_1\mathbf{f}^{(0)}; \quad x_0\mathbf{z}_b^{(1)} - x_1\mathbf{z}_b^{(0)}) \\ &:= \text{Com}_{ck}(\widehat{\mathbf{a}}; \widehat{\mathbf{r}}_a). \end{aligned} \quad (46)$$

Obviously, we have  $x_s\widehat{\mathbf{b}} + \widehat{\mathbf{a}} = y\mathbf{f}^{(s)}$  for  $s = \{0, 1\}$ . Taking each element in  $\widehat{\mathbf{b}} = (\widehat{b}_{j,i})_{i=0, j=0}^{\beta-1, k-1}$  and  $\widehat{\mathbf{a}} = (\widehat{a}_{j,i})_{i=0, j=0}^{\beta-1, k-1}$ , we have the following system for all  $i \in [0, \beta), j \in [0, k)$ :

$$x_s\widehat{b}_{j,i} + \widehat{a}_{j,i} = yf_{j,i}^{(s)}. \quad (47)$$

Taking  $\sum_{i=0}^{\beta-1} f_{j,i}^{(s)} = x_s$  and Equation (47), we have

$$yx_s = \sum_{i=0}^{\beta-1} yf_{j,i}^{(s)} = \sum_{i=0}^{\beta-1} x_s\widehat{b}_{j,i} + \sum_{i=0}^{\beta-1} \widehat{a}_{j,i}, \quad (48)$$

and thus

$$0 = x_s \left( \sum_{i=0}^{\beta-1} \widehat{b}_{j,i} - y \right) + \sum_{i=0}^{\beta-1} \widehat{a}_{j,i}. \quad (49)$$

Based on the  $\gamma$ -binding property of the commitment scheme, Equation (49) holds for  $s = \{0, 1\}$ . Therefore, we have  $\sum_{i=0}^{\beta-1} \widehat{b}_{j,i} - y = 0$  and  $\sum_{i=0}^{\beta-1} \widehat{a}_{j,i} = 0$ , and thus  $\sum_{i=0}^{\beta-1} \widehat{b}_{j,i} = y$ , i.e.,  $\sum_{i=0}^{\beta-1} \widehat{b}_{j,i} = y \sum_{i=0}^{\beta-1} b_{j,i}$  for  $\sum_{i=0}^{\beta-1} b_{j,i} = 1$ . Based on step 23, we have  $b_{j,0} = 1 - \sum_{i=1}^{\beta-1} b_{j,i}$ . Thus,  $\|b_{j,0}\| \leq 1 + 4\phi_1 \sqrt{kd(\beta-1)} \approx 4\phi_1 \sqrt{kd\beta}$ .

Now we construct  $b_i$ 's for all  $i \in [0, N)$  with  $b_i = \prod_{j=0}^{k-1} b_{j,i_j}$ , where  $i_j$ 's are the digits of representation of  $i$  in base  $\beta$  such that  $i = (i_0, \dots, i_{k-1})$ . Clearly,  $b_i \neq 0$  if and only if  $b_{j,i_j} \neq 0$  for all  $j \in [0, k)$ .

Based on Equation (45) and Lemma 6, we have

$$\begin{aligned} \|b_i\| &= \left\| \prod_{j=0}^{k-1} b_{j,i_j} \right\| \leq d^{\frac{k-1}{2}} \prod_{j=0}^{k-1} \|b_{j,i_j}\| \\ &\leq d^{\frac{k-1}{2}} \|b_{j,0}\|^k \leq (4\phi_1 \sqrt{kd\beta})^k d^{k-\frac{1}{2}} = \gamma_{LS}. \end{aligned} \quad (50)$$

Considering the  $\gamma$ -binding property of the commitment scheme, the following equation holds for  $(k+1)$  challenges

$$y f_{j,i}^{(s)} = x_s \widehat{b}_{j,i} + \widehat{a}_{j,i} = y x_s b_{j,i} + \widehat{a}_{j,i}, \quad s \in [0, k]. \quad (51)$$

We compute  $\widehat{p}_i(x_s) = y^k \prod_{j=0}^{k-1} f_{j,i_j}^{(s)} = \prod_{j=0}^{k-1} (y x_s b_{j,i_j} + \widehat{a}_{j,i_j})$  for each  $i \in [0, N)$ . Obviously, for all  $s \in [0, k]$ , if  $\widehat{p}_i(x_s)$  is a polynomial of degree  $k$ , then  $b_{j,i_j} \neq 0$  for all  $j \in [0, k)$ , which indicates  $b_i \neq 0$ . Thus, for all  $i \in [0, \beta)$ , we have at least one  $b_i$  is not zero, i.e.,  $\|\mathbf{b}\| > 0$ .

As the last verification step holds, we multiply both sides of the equation by  $y^k$ :

$$\begin{aligned} &\sum_{i=0}^{N-1} \widehat{p}_i(x_s) \cdot P_i - \sum_{j=0}^{k-1} y^k E_j x_s^j \\ &= x_s^k y^k \sum_{i=0}^{N-1} P_i + \sum_{j=0}^{k-1} E'_j x_s^j = \text{Com}_{ck}(\mathbf{0}; y^k \mathbf{z}_r^{(s)}), \end{aligned} \quad (52)$$

where  $E'_j$ 's are the terms multiplied by the monomials  $x_s^j$ 's of degree at most  $(k-1)$  and are independent from  $x_s$ . Taking all  $(k+1)$  transcripts, we have

$$\begin{pmatrix} 1 & x_0 & \cdots & x_0^k \\ 1 & x_1 & \cdots & x_1^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \cdots & x_k^k \end{pmatrix} \cdot \begin{pmatrix} E'_0 \\ E'_1 \\ \vdots \\ y^k \sum_{i=0}^{N-1} b_i P_i \end{pmatrix} = \begin{pmatrix} \text{Com}_{ck}(\mathbf{0}; y^k \mathbf{z}_r^{(0)}) \\ \text{Com}_{ck}(\mathbf{0}; y^k \mathbf{z}_r^{(1)}) \\ \vdots \\ \text{Com}_{ck}(\mathbf{0}; y^k \mathbf{z}_r^{(k)}) \end{pmatrix}. \quad (53)$$

Let the Vandermonde matrix on the left hand side of Equation (53) be  $\mathbf{V}$ . Based on Equation (6), we can obtain  $(\mathbf{0}, y^k \widehat{\mathbf{r}})$  as the opening of  $\det(\mathbf{V}) \cdot y^k \sum_{i=0}^{N-1} b_i P_i$ ,

where  $\widehat{\mathbf{r}} = \sum_{i=0}^{N-1} \Gamma_i \mathbf{z}_r^{(i)}$  ( $\Gamma_i$  is defined in Equation (4)). Based on Lemma 9, we have

$$\begin{aligned}
& \det(\mathbf{V}) \cdot y^k \sum_{i=0}^{N-1} b_i P_i = \text{Com}_{ck}(\mathbf{0}; y^k \widehat{\mathbf{r}}) \\
\implies & y^k \left( \det(\mathbf{V}) \cdot \sum_{i=0}^{N-1} b_i P_i - \text{Com}_{ck}(\mathbf{0}; \widehat{\mathbf{r}}) \right) = 0 \\
\implies & y \left( \det(\mathbf{V}) \cdot \sum_{i=0}^{N-1} b_i P_i - \text{Com}_{ck}(\mathbf{0}; \widehat{\mathbf{r}}) \right) = 0 \\
\implies & \det(\mathbf{V}) \cdot y \sum_{i=0}^{N-1} b_i P_i = \text{Com}_{ck}(\mathbf{0}; y \widehat{\mathbf{r}}) = 0.
\end{aligned} \tag{54}$$

Thus we extract an opening of  $\det(\mathbf{V}) \cdot y \sum_{i=0}^{N-1} b_i P_i$  as  $(\mathbf{0}, y \widehat{\mathbf{r}})$ . Let  $\kappa = k(k+1)/2$  and  $\kappa' = k(k-1)/2$ . Based on Lemma 1 and Lemma 4, we have the bound of  $\|y \widehat{\mathbf{r}}\|$ :

$$\begin{aligned}
\|y \widehat{\mathbf{r}}\| & \leq (k+1)d(2p)^{\kappa'+1} w^{\kappa'} \cdot 2\phi_2 T_2 \sqrt{md} \\
& \leq (k+1)2^{\kappa'+2} \sqrt{2}\phi_2 \mathcal{B} m d^2 w^\kappa p^{\kappa+1} = \gamma'_{LS}.
\end{aligned} \tag{55}$$

**SHVZK:** Assume that the protocol is not aborted. The simulator samples  $\mathbf{r} \leftarrow \{-\mathcal{B}, \dots, \mathcal{B}\}^{md}$ ,  $f_{j,i} \leftarrow D_{\phi_1 T_1}^d$  for all  $i \in (0, \beta)$  and  $j \in [0, k)$ ,  $\mathbf{z}_b, \mathbf{z}_r \leftarrow D_{\phi_2 T_2}^{md}$ ,  $E_j \leftarrow \mathcal{U}(R_q^n)$  for all  $j \in (0, k)$ , and sets  $B = \text{Com}_{ck}(\mathbf{0}; \mathbf{r})$ . Then, given  $x$ , it computes  $f_{j,0} = x - \sum_{i=1}^{\beta-1} f_{j,i}$  for all  $j \in [0, k)$  and sets  $\mathbf{f} = (f_{0,0}, \dots, f_{k-1, \beta-1})$ ,  $A = \text{Com}_{ck}(\mathbf{f}; \mathbf{z}_b) - xB$ , and  $E_0 = \sum_{i=0}^{N-1} (\prod_{j=0}^{k-1} f_{j,i_j}) P_i - \text{Com}_{ck}(\mathbf{0}; \mathbf{z}_r) - \sum_{j=1}^{k-1} E_j x^j$ . Obviously, the simulated transcript  $((A, B, (E_j)_{j=0}^{k-1}), x, (\mathbf{f}, \mathbf{z}_b, \mathbf{z}_r))$  will be an accepted transcript.

Based on Lemma 7, the distributions of  $\mathbf{f}$ ,  $\mathbf{z}_b$ ,  $\mathbf{z}_v$  are statistically close to the real distributions. The simulated distributions of  $A$  and  $E_0$  are the same as the real ones. Due to the hiding property of the commitment scheme, the distribution of simulated  $B$  is computationally indistinguishable from the real case. Finally, the simulated  $E_1, \dots, E_{k-1}$  are computationally indistinguishable from the real cases based on the M-LWE assumption.

Considering  $M$  inputs  $(a_i)_{i=0}^{M-1}$ . Let  $a = \sum_{i=0}^{M-1} a_i$ ,  $k = \lceil \log(a) \rceil$ , and  $a[j]$  be the  $j$ -th bit of  $a$  where  $0 \leq j < k$ . First, taking  $\sum_{i=0}^{M-1} a_i[0]$  and writing it as the binary representation  $(\tau_0^{(0)}, \dots, \tau_{k-1}^{(0)})$  such that  $\sum_{i=0}^{M-1} a_i[0] = \sum_{t=0}^{k-1} (\tau_t^{(0)} \cdot 2^t)$ , we have  $a[0] = \tau_0^{(0)}$ . Furthermore, taking  $\tau_1^{(0)}$  and  $\sum_{i=0}^{M-1} a_i[1]$ , we can write the sum of them as the binary representation  $(\tau_0^{(1)}, \dots, \tau_{k-1}^{(1)})$  and derive  $a[1] = \tau_0^{(1)}$ . In this way, we can observe that in order to derive  $a[j]$ , the  $j$ -th element consists of two parts:  $\sum_{i=0}^{M-1} a_i[j]$  and  $\sum_{t=1}^j \tau_t^{(j-t)}$  (the latter one is the sum of all carries from  $a[j-1], \dots, a[0]$ ). Thus, for all  $j \in [0, k)$ , writing  $\sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)}$  as the binary representation  $(\tau_0^{(j)}, \dots, \tau_{k-1}^{(j)})$ , we have

$$\sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} = \sum_{t=0}^{k-1} (\tau_t^{(j)} \cdot 2^t). \tag{56}$$

Obviously,  $a[j] = \tau_0^{(j)}$ . Thus, we have

$$a[j] = \sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t^{(j)} \cdot 2^t). \quad (57)$$

Similarly, let  $b = \sum_{i=0}^{S-1} b_i$ , we can derive the following equation for  $S$  outputs

$$b[j] = \sum_{i=0}^{S-1} b_i[j] + \sum_{t=1}^j \tau_t''^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t''^{(j)} \cdot 2^t), \quad (58)$$

when the balance property holds such that  $k = \lceil \log(a) \rceil = \lceil \log(b) \rceil$ . Taking Equation (61) and (62), for all  $j \in [0, k)$ , we have

$$\begin{aligned} b[j] - a[j] &= \sum_{i=0}^{S-1} b_i[j] - \sum_{i=0}^{M-1} a_i[j] \\ &+ \sum_{t=1}^j (\tau_t''^{(j-t)} - \tau_t^{(j-t)}) - \sum_{t=1}^{k-1} ((\tau_t''^{(j)} - \tau_t^{(j)}) \cdot 2^t) \\ &= \sum_{i=0}^{S-1} b_i[j] - \sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t^{(j)} \cdot 2^t), \end{aligned} \quad (59)$$

where  $\tau_t^{(j)} = \tau_t''^{(j)} - \tau_t^{(j)}$ . Obviously, the corrector value in [17] is a special case of Equation (63) under  $k = 2$  by regarding  $\tau_1^{(j-1)} = \tau_j$ ,  $\tau_1^{(j)} = \tau_{j+1}$ , and  $\tau_t^{(j-t)} = \tau_t^{(j)} = 0$  when  $t > 1$ .

As  $\tau_t''^{(j)}, \tau_t^{(j)} \in \{0, 1\}$ , we have  $\tau_t^{(j)} \in \{-1, 0, 1\}$ , which narrows down the range of corrector values in [17] (but requires more corrector values).

## D Security Reduction (Sketch) of Lemma 5 and Theorem 4

Lemma 5 and Theorem 4 reduces “forging a ring signature” to “finding an HMC collision” for ring signature unforgeability. The security game can be illustrated in Figure 8.

**Oracle Simulation.** The ring signature challenger  $\mathcal{A}_{T4}$  will forward these queries and responses between the HMC collision finder  $\mathcal{A}_{L5}$  and the ring signature forger  $\mathcal{F}_{T4}$ .  $\mathcal{A}_{L5}$  simulates the oracles as follows:

*Registration query.* Assume  $\mathcal{F}_{T4}$  can only query  $N$  times ( $N \geq 1$ ).  $\mathcal{A}_{L5}$  randomly picks  $l \leftarrow \{0, 1, \dots, N-1\}$ . For index  $l$ ,  $\mathcal{A}_{L5}$  sets  $P_l = \text{Com}_{ck}(1, 0, \dots, 0; \mathbf{r})$ . For other indices  $j \neq l$ ,  $\mathcal{A}_{L5}$  calls the RKeyGen algorithm to generate a public/private key pair  $(P_j, r_j)$ . Upon the  $(i+1)$ -th query,  $\mathcal{A}_{L5}$  returns the corresponding public key  $P_i$ .

*Corruption query.* On input a public key  $P_i$ ,  $\mathcal{A}_{L5}$  aborts when  $i = l$ . Otherwise,  $\mathcal{A}_{L5}$  returns the corresponding private key  $r_i$ .

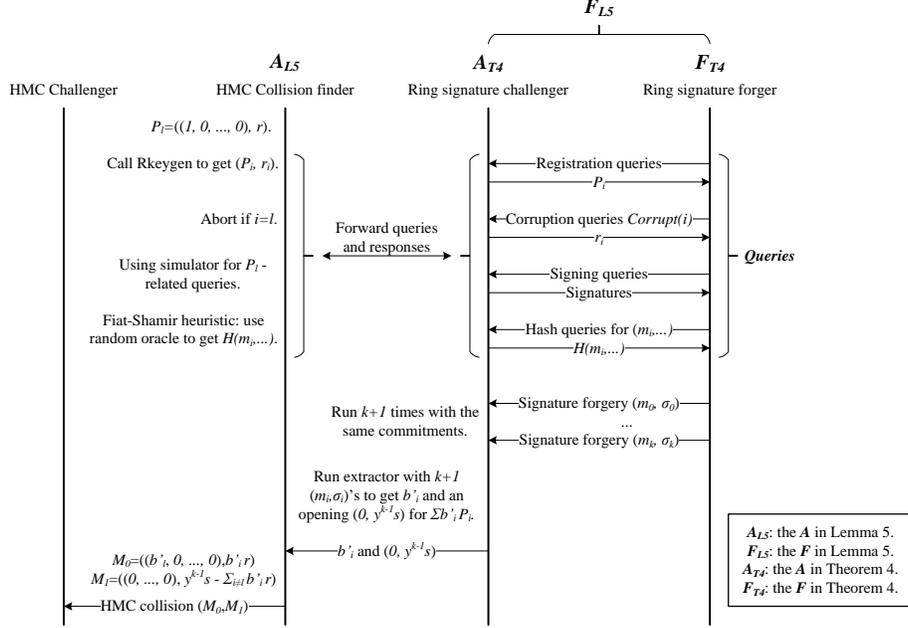


Fig. 8: Reduction from “forging a ring signature” to “finding an HMC collision” for ring signature unforgeability.

*Signing query.* When  $\mathcal{F}_{T4}$  queries to sign on message  $m_i$  with a signer  $P_i$  in a public key list  $\mathbf{P}_i = \{P_j | j \in \mathbf{t}_j\}$  where  $\mathbf{t}_i$  indicates the indices of the public keys in  $\{P_0, \dots, P_{N-1}\}$ , i.e.,  $\mathbf{t}_i \subset \{1, \dots, N-1\}$ ,  $\mathcal{A}_{L5}$  processes as follows:

- If  $i \neq l$ ,  $\mathcal{A}_{L5}$  calls RSign algorithm directly to get the corresponding signature since he has  $r_i$  and programs the Hash function (random oracle) if needed.
- If  $i = l$ ,  $\mathcal{A}_{L5}$  runs the simulator in the proof of Theorem 2 (SHVZK prosperity) get the signature and programs the Hash function (random oracle) so that  $H(ck, m_i, \mathbf{P}_i, A, B, (E_j)_{j=0}^{k-1}) = x$ .

*Hash query.* For queries with inputs that has already been programmed,  $\mathcal{A}_{L5}$  returns the corresponding output. Otherwise,  $\mathcal{A}_{L5}$  chooses  $x$  at random from the set  $\mathcal{C} \setminus \{x_0, \dots, x_{m-1}\}$  where  $x_i$ 's are the outputs of the Hash function that have been programmed. The output of the Hash function for this input is programmed to  $x$ .

**Signature Forgery.** At a given point,  $\mathcal{F}_{T4}$  finishes running and outputs a forgery  $(m_i, \sigma_i)$ . Since  $P_l$  cannot be distinguished from other  $P_i$ 's due to the hiding property of the HMC commiement scheme and  $\mathcal{F}_{T4}$  can only make  $N$  times of registration queries to  $\mathcal{A}_{L5}$ , we have the signature is signed by the signer  $P_l$  with non-negligible probability<sup>8</sup>, i.e.,  $b_l \neq 0$ .

<sup>8</sup> Other signers may also be involved such that  $b_i \neq 0$  for some  $i \neq l$ .

**Output.** After collecting  $k + 1$  signature forgeries with the same commitments (this can be done in polynomial time using the forking lemma),  $\mathcal{A}_{T4}$  computes  $b'_i$ 's and an opening  $(\mathbf{0}, y^{k-1}\mathbf{s})$  to  $\sum_{i=0}^{N-1} b'_i P_i$  by running the extractor in the proof of Theorem 2 ( $(k + 1)$ -special soundness) and forwards  $b'_i$ 's and  $(\mathbf{0}, y^{k-1}\mathbf{s})$  to  $\mathcal{A}_{L5}$ . Accordingly,  $\mathcal{A}_{L5}$  can find a collision for the HMC commitment scheme,  $M_0 = ((b'_l, 0, \dots, 0), b'_l \mathbf{r})$  and  $M_1 = (\mathbf{0}, y^{k-1}\mathbf{s} - \sum_{i \neq l} b'_i \mathbf{r}_i)$  since  $(b'_l, 0, \dots, 0) \neq \mathbf{0}$  ( $\mathbf{r}_i$ 's are the private keys of other users in the ring).

## E An Alternative Approach to Reduce the Cost of Corrector Values

We present an alternative approach to reduce the cost of corrector values in [17] by narrowing down the range of corrector values to  $\{-1, 0, 1\}$ . Based on the discussion in Section 9, we can avoid the cost of UMC in range proofs.

Considering  $M$  inputs  $(a_i)_{i=0}^{M-1}$ . Let  $a = \sum_{i=0}^{M-1} a_i$ ,  $k = \lceil \log(a) \rceil$ , and  $a_i[j]$  be the  $j$ -th bit of  $a_i$  where  $0 \leq j < k$ . First, taking  $\sum_{i=0}^{M-1} a_i[0]$  and writing it as the binary representation  $(\tau_0^{(0)}, \dots, \tau_{k-1}^{(0)})$  such that  $\sum_{i=0}^{M-1} a_i[0] = \sum_{t=0}^{k-1} (\tau_t^{(0)} \cdot 2^t)$ , we have  $a[0] = \tau_0^{(0)}$ . Furthermore, taking  $\tau_1^{(0)}$  and  $\sum_{i=0}^{M-1} a_i[1]$ , we can write the sum of them as the binary representation  $(\tau_0^{(1)}, \dots, \tau_{k-1}^{(1)})$  and derive  $a[1] = \tau_0^{(1)}$ . In this way, we can observe that in order to derive  $a[j]$  (the  $j$ -th bit of  $a = \sum_{i=0}^{M-1} a_i$ ), the  $j$ -th element consists of two parts:  $\sum_{i=0}^{M-1} a_i[j]$  and  $\sum_{t=1}^j \tau_t^{(j-t)}$  (the latter one is the sum of all carries from  $a[j-1], \dots, a[0]$ ). Thus, for all  $j \in [0, k)$ , writing  $\sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)}$  as the binary representation  $(\tau_0^{(j)}, \dots, \tau_{k-1}^{(j)})$ , we have

$$\sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} = \sum_{t=0}^{k-1} (\tau_t^{(j)} \cdot 2^t). \quad (60)$$

Obviously,  $a[j] = \tau_0^{(j)}$ . Thus, we have

$$a[j] = \sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t^{(j)} \cdot 2^t). \quad (61)$$

Similarly, let  $b = \sum_{i=0}^{S-1} b_i$ , we can derive the following equation for  $S$  outputs

$$b[j] = \sum_{i=0}^{S-1} b_i[j] + \sum_{t=1}^j \tau_t''^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t''^{(j)} \cdot 2^t), \quad (62)$$

when the balance property holds such that  $k = \lceil \log(a) \rceil = \lceil \log(b) \rceil$ . Taking Equation (61) and (62), for all  $j \in [0, k)$ , we have

$$\begin{aligned}
b[j] - a[j] &= \sum_{i=0}^{S-1} b_i[j] - \sum_{i=0}^{M-1} a_i[j] \\
&+ \sum_{t=1}^j (\tau_t''^{(j-t)} - \tau_t'^{(j-t)}) - \sum_{t=1}^{k-1} \left( (\tau_t''^{(j)} - \tau_t'^{(j)}) \cdot 2^t \right) \\
&= \sum_{i=0}^{S-1} b_i[j] - \sum_{i=0}^{M-1} a_i[j] + \sum_{t=1}^j \tau_t^{(j-t)} - \sum_{t=1}^{k-1} (\tau_t^{(j)} \cdot 2^t),
\end{aligned} \tag{63}$$

where  $\tau_t^{(j)} = \tau_t''^{(j)} - \tau_t'^{(j)}$ . Obviously, the corrector value in [17] is a special case of Equation (63) under  $k = 2$  by regarding  $\tau_1^{(j-1)} = \tau_j$ ,  $\tau_1^{(j)} = \tau_{j+1}$ , and  $\tau_t^{(j-t)} = \tau_t^{(j)} = 0$  when  $t > 1$ .

As  $\tau_t''^{(j)}, \tau_t'^{(j)} \in \{0, 1\}$ , we have  $\tau_t^{(j)} \in \{-1, 0, 1\}$ , which narrows down the range of corrector values in [17] (but requires more corrector values).