IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 29, 2019, accepted January 14, 2020, date of publication January 20, 2020, date of current version January 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967789

On Design of Single-Layer and Multilayer Code-Based Linkable Ring Signatures

YAN REN[1], QIUXIA ZHAO[1], HAIPENG GUAN[1], AND ZHIQIANG LIN[2]
[1]School of Mathematics and Information Technology, Yuncheng University, Yuncheng 044000, China
[2]School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

Corresponding author: Zhiqiang Lin (linzhiqiang0824@163.com)

This work was supported in part by the National Natural Science Foundation of Shanxi under Grant 201601D021014, in part by the Higher Education Technology Innovation Projects Foundation of Shanxi under Grant 2019L0860, in part by the National Natural Science Foundation of China under Grant 61702124, and in part by the Subject Research Projects Foundation of Key Laboratory of Information Security Technology of Guangdong under Grant GDXXAQ2016-05.

ABSTRACT In this paper, we present an effective code-based linkable ring signature scheme based on Borromean ring signature. The security of the scheme is based on the hardness of Syndrome Decoding problem, General Syndrome Decoding problem and Codeword Finding problem. We prove that our scheme has all the properties that a linkable ring signature scheme should have: unforgeability, anonymity, linkability and non-slanderability. Efficiency analysis shows that our scheme has a smaller signature size than the existing scheme under the same security conditions. Furthermore, this signature scheme can be easily extended to multiple layers. That is, code-based multilayer linkable ring signature scheme can be obtained and used for transactions with multiple inputs.

INDEX TERMS Post-quantum, ring signature, linkable ring signature, code-based cryptography.

I. INTRODUCTION

A. BACKGROUND

Blockchain has been widely used in many fields since its introduction in 2008 [1]–[5], but there are still many problems that restrict its development. Such as, how to protect user's privacy how to prevent double spending. Recent research indicates that linkable ring signature scheme can solve these two problems well.

Ring signature, which was first introduced by Rivest in [6], is a technique for anonymously revealing reliable messages. It can be seen as a simplified group signature scheme without group administrator, establishment and member revocation process. The member's information in the ring is a part of the final signature result. In a ring signature scheme, the signer first selects a temporary set of signers, including the signer itself. User can sign with his private key and the public key of other members of the ring without the consent of other members. The verifier is able to confirm that the signature is from a ring, but do not know who is the real signer. It is well known that the user's anonymity is achieved.

Later, linkable ring signature was proposed in [7]. A linkable ring signature scheme that must satisfy the linkability. It means that, if the signer signs two messages using the same private key, he will be found. This property can be used to guarantee the prevention of double spending.

Monero has used this anonymity and linkability in cryptocurrencies to prevent double spending and protect user's privacy [8], [9]. The security of their scheme is based on the discrete logarithm problem of elliptic curves. As everyone knows, many cryptographic schemes based on classical number theory are suffered from future quantum computer's threats [10]. Therefore, it is very meaningful to study the construction of post-quantum linkable ring signature scheme. Currently post-quantum signature research is mostly focused on four different approaches: hash-based, multivariate-based, code-based, and lattice-based. Authors in [11] proposed a linkable ring signature scheme with stealth addresses (SALRS). This scheme enables both payer and payee of the transaction to be hidden in the cryptocurrency. In this paper, we focus on construction of code-based linkable ring signature scheme.

B. OUR CONTRIBUTION

Using the same structure as Monero's in [8], [9], we present an effective code-based linkable ring signature scheme based on Borromean ring signature [12]. In our scheme, we use an exact indistinguishable distribution to generate signature.

The associate editor coordinating the review of this manuscript and approving it for publication was Donghyun Kim.

TABLE 1. Signature size compare.

Number of user	[13]	ours($q = 2^8$)	ours($q = 2^{32}$)	ours($q = 2^{64}$)	ours($q = 2^{128}$)
$2^6 users$	2496	$\approx 79.87KB$	$\approx 319.48KB$	$\approx 638.96KB$	$\approx 1277.92KB$
$2^8 users$	9984	$\approx 317.62KB$	$\approx 1270.48KB$	$\approx 2540.96KB$	$\approx 5081.92KB$
$2^{10} users$	39936	$\approx 1268.62KB$	$\approx 5074.48KB$	$\approx 10148.96KB$	$\approx 20297.92KB$

At the same time, the signature size of this scheme is linear in number of user N and the size of q in finite field. Analysis shows that our scheme has a smaller signature size under the same security conditions. A comparison is given in Table 1 below.

Furthermore, the scheme we proposed can be easily extended to multiple layers. We also present a code-based multilayer linkable ring signature scheme which can be used for transactions with multiple inputs.

C. ORGANIZATION OF THIS PAPER

The rest of the paper is organized as follows. In section 2, we introduce some preliminary results including the definition and security model of linkable ring signature. Coed-based linkable ring signature, the main contribution of this paper will be described in section 3. Coed-based multilayer linkable ring signature is given in section 4. In section 5, a formal security prove for our schemes will be presented. We conclude this work by analyzing the signature size of our scheme.

II. RELATED WORK

Since the (linkable) ring signature was introduced, many schemes have been proposed. These schemes can divide into classic (linkable) ring signature schemes and post-quantum (linkable) ring signatures schemes. In this paper, we mainly focus on code-based linkable ring signature schemes, so we introduce some research progress on classical (linkable) ring signatures and code-based (linkable) ring signatures.

A. CLASSICAL (LINKABLE) RING SIGNATURES

There are many (linkable) ring signature schemes rely on the hardness problems of number-theoretic. Here we only list some of them, such as the schemes in [14]–[26]. Some of these schemes have specific application scenarios, such as the schemes in [16] and [17] are based on certificates and identity-based, respectively. The signature size in [6], [20], [24]–[26] is linear with the number of signers. The scheme in [18] is a linkable version of [27], retains the constant size signature.

B. CODE-BASED (LINKABLE) RING SIGNATURES

Code-based ring signatures were first introduced in 2007 [28]. Then, some code-based ring signature schemes and many other variants have been proposed have been proposed [29]–[32]. Such as, schemes in [29], [30] are threshold ring signature. Reference [32] proposed an undeniable signature scheme.

Code-based linkable ring signatures were first introduced in [13]. They construct code-based linkable ring signature by using the Fiat-Shamir transform. The GStern's protocol need repeated 140 time in their scheme. It makes the signature size so large.

III. PRELIMINARIES

In this section, we give some preliminary results as well as the definition and security model of linkable ring signature.

A. HAMMING DISTANCE, WEIGHT

Definition 1 (Hamming Distance, Weight): Hamming distance $d(u, v)$ of two words $u = u_1, u_2, \ldots u_n$ and $v = v_1, v_2, \ldots v_n$ is the number of different components of u and v. That is, $d(u, v) =| i : u_i \neq v_i |$. The Hamming weight $w(u)$ of the word u is the Hamming distance between u and 0, where 0 is a word containing n $0's$.

B. HARD PROBLEMS

We first present 3 NP-complete problems: the Syndrome Decoding, General Syndrome Decoding and Codeword Finding assumption, which will be used for the subsequent scheme constructed [33].

Definition 2 (Syndrome Decoding (SD) Problem): Given random A is a $(n-k) \times n$ matrix over F_q, $S \in F_q^{n-k}$ and an integer $t > 0$, find a vector $e \in F_q^n$ with $w(e) \leq t$, such that $Ae = S$ where $w(e)$ is the Hamming weight of e and t is a positive integer.

Definition 3 (General Syndrome Decoding problem): Given random $A, B \in F_q^{n\times(n-k)}$, $S, T \in F_q^{n-k}$ and an integer $t > 0$, find a vector $e \in F_q^n$ with $w(e) \leq t$, such that $Ae = S$ and $Be = T$, where $w(e)$ is the Hamming weight of e and t are positive integers.

Definition 4 (Codeword Finding (CF) Problem): Given a random matrix $A \in F_q^{(n-k)\times n}$ and an integer $t > 0$, find a non-zero vector $e \in F_q^n$ with $w(e) \leq t$, such that $Ae = 0$.

C. LINKABLE RING SIGNATURE

The syntax of a linkable ring signature can be seen in [7], [26]. There are five algorithms in a linkable ring signature scheme.

Definition 5 (Linkable Ring Signature):

1) ***Setup:*** *The input to this algorithm is a security parameter and outputs the public parameters.*
2) ***KeyGen:*** *The input to this algorithm is public parameter and outputs the user's public key and private key.*
3) ***Sign:*** *The input to this algorithm is the public parameter, message m, signer's private key, user's public key list and outputs the signature.*

4) ***Verify:*** *The input to this algorithm is the signature on message m and outputs $b \in \{0, 1\}$. 1 and 0 indicate that the signature is a valid signature or an invalid signature respectively.*
5) ***Link:*** *The input to this algorithm is two signatures on two messages and outputs 0 or 1.*

D. SECURITY MODEL OF LINKABLE RING SIGNATURE

A secure linkable ring signature must be correctness, unforgeable, anonymous, linkable and non-slanderable. The security model of linkable ring signature we adopt is based on [34].

Definition 6 (Correctness): The signature, generated by the legal signer after executes the signature algorithm correctly, can pass the verification algorithm with probability 1.

In the following definitions, we use $L = \{pk_i \mid i \in [1, N]\}$ to denote the list of the public keys of users in the signature scheme and need to assume four oracles named join oracle O_J, key generation oracleO_K, signature oracle O_S, and hash oracle O_H.

- O_J: On input a new user join request, outputs pk_i for new user.
- O_K: On input a pk_i, outputs the corresponding sk_i.
- O_S: On input a public key set $L = \{pk_1, pk_2, \ldots, pk_N\}$, where pk_i is generated by O_K, a message m, outputs a valid signature σ'.
- O_H: Outputs a hash value.

We use S, C to denote the simulator and adversary. C is given the access to O_J, O_K, O_S and O_H. The unforgeability, anonymity, linkablility and non-slanderability for linkable ring signature are defined by the following games between a simulator S and an adversary C. In the following description $param.$ denotes system parameter.

Unforgeability:

Considered Game 1, as shown in TABLE 2, C first generates a signature for message m using a public key list L obtained from S, calls the verify algorithm and gets an output b.

TABLE 2. Game for unforgeability.

Game 1:
1. S: $param. \leftarrow Setup(1^\lambda)$
2. S: $L \leftarrow KeyGen(1^k, param.)$
3. C : $\sigma_L(m) \leftarrow Sign(L, m)$
4. $b \leftarrow Verify(L, m, \sigma)$

C wins Game 1 if the following conditions are met:

- The output of b is 1.
- All public keys in L are the outputs of O_J
- Adversary C only make query for $pk_i \notin L$.
- (L, m) was not required to sign.

We define

$$Adv_C^{unf} = Pr[b = 1].$$

Definition 7: The linkable ring signature is unforgeable if for all PPT adversarys C, Adv_C^{unf} is negligible.

TABLE 3. Game for anonymity.

Game 2:
1. C: $(pk_0, pk_1) \leftarrow O_J$
2. C: sends (pk_0, pk_1, m) to S
3. S: $b \leftarrow \{0, 1\}$
4. S:$\sigma_b(m) \leftarrow Sign(pk_0, pk_1, m)$
5. S: computes $\sigma_b(m)$ and sends it to C
6. C: computes b'

Anonymity:

Anonymity means that it is impossible for adversary to distinguish the signer's pk with probability 1/2. We consider game for anonymity as shown in TABLE 3.

C wins Game 2 if the following conditions are met:

- pk_0 and pk_1 cannot be used in O_K and O_S.
- When $b = b'$, output 1 with a probability $\frac{1}{2}$.

We define

$$Adv_C^{ano} = Pr[b = b'] - \frac{1}{2}.$$

Definition 8: The linkable ring signature is anonymous if for all PPT adversaries C, Adv_C^{ano} is negligible.

Linkability:

Linkability means that if there are two valid linkable ring signatures which were correctly generated with same sk, it should be linked for adversary C. We describe this Game as presented in TABLE 4.

TABLE 4. Game for linkability.

Game 3:
1. S: $param. \leftarrow Setup(1^\lambda)$
2. S: $L \leftarrow KeyGen(1^k, param.)$
3. C: $\sigma_L(m) \leftarrow Sign(L, m, sk)$
4. C: $\sigma'_{L'}(m') \leftarrow Sign(L', m', sk)$
5. $b \leftarrow Verify(L, m, \sigma_L(m))$
6. $b' \leftarrow Verify(L', m', \sigma'_{L'}(m'))$
7. $c \leftarrow Link(\sigma_L(m), \sigma'_{L'}(m'))$

C wins Game 3 if the following conditions are met:

- C just can make O_K query once and obtain private key sk_i corresponding to the public key pk_i.
- $b = b' = 1$.
- $c = 0$.

We define

$$Adv_C^{ano} = Pr[C \text{ wins Game 3}].$$

Definition 9: The linkable ring signature is anonymous if for all PPT adversaries C, Adv_A^{ano} is negligible.

Non-slanderability:

Non-slanderability means that an adversary cannot frame an honest user for producing a signature linked with another signature not signed by the user. That is, if there are two valid linkable ring signatures which were correctly generated with different $sk's$, they should be unlinked.

TABLE 5. Game for non-slanderability.

Game 4:
1. S: $param. \leftarrow Setup(1^{\lambda})$ 2. S: $L \leftarrow (1^k, param.)$ 3. C: $(pk_\pi, sk_\pi) \leftarrow O_K$, 4. C: sends (pk_π, sk_π) to S 5. S: $\sigma_L(m) \leftarrow O_S(L, m, sk_\pi)$ 6. S: sends $\sigma_L(m)$ to C 7. C: $\sigma'_{L'}(m') \leftarrow O_S(L', m')$ 8. $b \leftarrow Verify(L', m', \sigma'_{L'}(m'))$ 9. $c \leftarrow Link(\sigma_L(m), \sigma'_{L'}(m'))$

C wins Game 4 if the following conditions are met:

- The generation process of $\sigma'_L(m)$ does not use pk_π and sk_π.
- $b = 1$.
- $c = 1$.

We define

$$Adv_C^{N-s} = Pr[C \text{ wins Game 4}].$$

Definition 10: The linkable ring signature is anonymous if for all PPT adversarys C, Adv_C^{N-s} is negligible.

IV. CODE-BASED LINKABLE RING SIGNATURE SCHEME

In this section, we will give the construction of our code-based ring signature scheme.

There are five algorithms named (*Setup*, *KeyGen*, *Sign*, *Verify*, *Link*) in our code-based linkable ring signature scheme, which described as follows.

A. SETUP

The input of the setup is an security parameter λ, outputs are $n, k, t \in N_+$, such that $n > k, A, B \leftarrow F_q^{(n-k)\times n}$. We use $w(*)$ to denote the Hamming weight of $*$. $H : H(\cdot) \rightarrow F_q$ is a hash function.

B. KEYGEN

The inputs of the KeyGen algorithm is the public parameters, then it outputs the private-key and public-key for each user P_i as follow.

- Pick $e_i \leftarrow F_q^n$ such that $w(e_i) \leq t$.
- Compute $PK_i = Ae_i$.

Then the public key is PK_i and the private key is e_i.

C. SIGN

Assuming that the selected set is $S = \{1, 2, \ldots, N\}$ and the $\pi \in S$ is the true signer. The input of the Sign algorithm is the private key e_π, message m, the set of user's public key list $L = \{PK_i \mid i = 1, 2, \cdots, N\}$ and the public parameters A, B. The output of this algorithm is the signature σ. The details are described below:

- Calculate $T_\pi = Be_\pi$.
- Choose $u \leftarrow F_q^n$ with $w(u) \leq t$ uniform randomly.
- Calculate

$$d_{\pi+1} = H(L, T_\pi, m, Au, Bu).$$

For $i = \pi + 1, \pi + 2, \ldots, 1, 2, \ldots, \pi - 1$

1) Choose $c_i \leftarrow F_q, r_{i1}, r_{i2} \leftarrow F_q^n$ with $w(r_{ij}) \leq t, (j = 1, 2)$ uniform randomly.
2) Calculate $r_{z,i} = r_{i1} + c_i r_{i2}$.
3) Calculate

$$d_{i+1} = H(L, T_\pi, m, t_{i,1}, t_{i,2}),$$

where

$$t_{i,1} = Ar_{z,i} - d_i PK_i,$$
$$t_{i,2} = Br_{z,i} - d_i T_\pi.$$

4) Calculate

$$r_{z,\pi} = u + d_\pi e_\pi.$$

The signature is $\sigma = (d_1, (r_{z,i}), T_\pi)$.

D. VERIFY

1) For $i = 1, 2, \ldots, N$, compute

$$t'_{i,1} = Ar_{z,i} - d_i PK_i,$$
$$t'_{i,2} = Br_{z,i} - d_i T_\pi,$$
$$d'_{i+1} = H(L, T_\pi, m, t'_{i,1}, t'_{i,2}).$$

2) If $d_1 = H(L, T_\pi, m, t'_{N,1}, t'_{N,2}) = d_{N+1}$ output 1, else output 0.

E. LINK

Given two valid signatures for different message,

$$\sigma = (d_1, (r_{z,i}), T_\pi),$$
$$\sigma' = (d'_1, (r'_{z,i}), T'_\pi).$$

If $T_\pi = T'_\pi$, return 1, we claim that both signatures are come from the same user. Otherwise return 0.

V. MULTILAYER CODE-BASED LINKABLE RING SIGNATURE SCHEME

The proposed scheme in section IV can be extended to a multilayer linkable ring signature scheme, which are applied for confidential transactions with multiple inputs. We take a voting problem as an instance. An institution organizes a voting system that uses a multiple vote, the voter can vote for any subset of the alternatives. So, a voter might vote for Alice, Bob, and Charlie, rejecting Daniel and Emily. In order to protect the privacy of voters and prevent secondary voting, this voting can be organized in the blockchain and implemented through a multilayer linkable ring signature scheme. Regarding voting result for each candidate as an input, the voter can choose a ring member set $\{1, 2, \ldots, N\}$ among all voters to generate a linkable ring signature scheme using different private keys. In this way, the privacy of voters can be protected, and when voters vote twice on any candidate, they will be discovered through linkability.

We assume that each user has M secret keys to sign and propose a scheme with a set of $N \cdot M$ keys. The definition of linkability and the construction of the new multilayer linkable ring signature is presented below.

Definition 11 (Linkability): If any private keys $e_{\pi,j}$ used in two different signature, then these signatures would be linked.

Remark 1: In our multilayer linkable ring signature, we require $i \in \{1, 2, \ldots, N\}$ and $j \in \{1, 2, \ldots, M\}$.

A. SETUP

The input of the setup is an security parameter λ, outputs are $n, k, t \in N$, such that $n > k$, $A, B \leftarrow F_q^{(n-k)\times n}$. We use $w(*)$ to denote the Hamming weight of $*$. $H : H(\cdot) \rightarrow F_q$ is a hash function.

B. KEYGEN

The inputs of the Key Generation algorithm is the public parameters, then it outputs the private-key and public-key for each P_{ij} for $i \in \{1, 2, \ldots, N\}$ and $j \in \{1, 2, \ldots, M\}$ as follow. The subscript i indicates the $i - th$ user and j indicates the user's $j - th$ secret key.

- Pick $e_{ij} \leftarrow F_q^n$ such that $w(e_{ij}) \leq t$.
- Compute $PK_{ij} = Ae_{ij}$.

Then the public keys are PK_{ij} and the private keys are e_{ij}.

C. SIGN

Assuming that the selected set is $S = \{1, 2, \ldots, N\}$ and the $\pi \in S$ is the true signer. The input of the *Sign* algorithm is the private key $e_{\pi,j}$, message m, the set of user's public key list $L = \{PK_{ij}\}$, and the public parameters A, B. The output of this algorithm is the signature σ. The details are described below:

- Calculate $T_j = Be_{\pi,j}$ for all $j \in \{1, 2, \ldots, M\}$.
- Choose $u_j \leftarrow F_q^n$ with $w(u_j) \leq t$ uniform randomly.
- Calculate $d_{\pi+1} = H(L, T_{\pi,j}, m, Au_1, Au_2, \ldots, Au_M, Bu_1, Bu_2, \ldots, Bu_M)$.

1) For $i = \pi + 1, \pi + 2, \ldots, 1, 2, \ldots, \pi - 1$,
   a) Choose $c_{ij} \leftarrow F_q$, $r_{ij}^1, r_{ij}^2 \leftarrow F_q^n$ with $w(r_{ij})^h \leq t$, $(h = 1, 2)$ uniform randomly.
   b) Calculate $r_{i,j} = r_{ij}^1 + c_{ij}r_{ij}^2$, $i \neq \pi$.
   c) Calculate
   $$d_{i+1} = H(L, T_j, m, t_{i,j}^1, t_{i,j}^2),$$
   where
   $$t_{i,j}^1 = Ar_{i,j} - d_i PK_{i,j},$$
   $$t_{i,j}^2 = Br_{i,j} - d_i T_j.$$
2) For $i = \pi$, calculate
$$r_{\pi,j} = u_j + d_\pi e_{\pi,j}.$$

The signature is $\sigma = (d_1, (r_{i,j}), T_j)$.

D. VERIFY

1) For $i = 1, 2, \ldots, N$, compute
$$(t'_{i,j})^1 = Ar_{i,j} - d_i PK_{i,j},$$
$$(t'_{i,j})^2 = Br_{i,j} - d_i T_j,$$
$$d'_{i+1} = H(L, T_j, m, (t'_{i,j})^1, (t'_{i,2})^2).$$
2) If $d'_1 = d_1$ output 1, else output 0.

E. LINK

Given two valid signatures for different message,
$$\sigma = (d_1, (r_{i,j}), T_j)$$
$$\sigma' = (d'_1, (r'_{i,j}), T'_j)$$
If $T_j = T'_j$, return 1, we claim that both signatures are come from the same private key. Otherwise return 0.

VI. CORRECTNESS AND SECURITY ANALYSIS

In this section, we present the correctness and security of our schemes. We prove that our schemes have the usual properties for a linkable ring signature. Such as unforgeability, anonymity, linkability and non slanderability. Because the multi-layered scheme is an extension of the single-layer scheme, we just give proof of the single-layer scenario. The proof of the multi-layer case is similar.

A. CORRECTNESS ANALYSIS

Theorem 1: The verify process is correct.

Proof: For code-based linkable ring signature, the verify algorithm works as following:

1) If $i \neq \pi$, then d'_{i+1} can be obtained by the *Sign* algorithm.
2) if $i = \pi$, then
$$\begin{aligned} t'_{\pi,1} &= Ar_{z,\pi} - d_\pi PK_\pi \\ &= A(u + d_\pi e_\pi) - d_\pi Ae_\pi \\ &= Au + Ad_\pi e_\pi - d_\pi Ae_\pi \\ &= Au \\ t'_{\pi,2} &= Br_{z,\pi} - d_\pi T_\pi \\ &= B(u + d_\pi e_\pi) - d_\pi Be_\pi \\ &= Bu + Bd_\pi e_\pi - d_\pi Be_\pi \\ &= Bu \end{aligned}$$
So, in this case $d'_{i+1} = d_{i+1}$ holds.

For multilayer code-based linkable ring signature, the verify algorithm works as following:

1) If $i \neq \pi$, then d'_{i+1} can be obtained by the *Sign*. algorithm.
2) if $i = \pi$, then
$$\begin{aligned} (t'_{\pi,j})^1 &= Ar_{\pi,j} - d_{\pi,j} PK_{\pi,j} \\ &= A(u_j + d_{\pi,j} e_{\pi,j}) - d_{\pi,j} Ae_{\pi,j} \\ &= Au_j + Ad_{\pi,j} e_{\pi,j} - d_{\pi,j} Ae_{\pi,j} \\ &= Au_j \\ (t'_{\pi,j})^2 &= Br_{\pi,j} - d_{\pi,j} T_j \\ &= B(u_j + d_{\pi,j} e_{\pi,j}) - d_{\pi,j} Be_{\pi,j} \\ &= Bu_j + Bd_{\pi,j} e_{\pi,j} - d_{\pi,j} Be_{\pi,j} \\ &= Bu_j \end{aligned}$$
In other words, it holds also that $d'_{i+1} = d_{i+1}$.

In conclusion, the verification process is correct. □

Theorem 2: The linkabile process is correct. It means that if an honest user π generates signatures for two different messages use the same public key list, which can pass the verify algorithm, then the link-ability tags must equal.

Proof: Suppose an honest user π generates signatures for two different messages m, m' by using the different public key list L, L' and same private key. And both the signature can pass the *verify* algorithm. The link-ability tags are T_π, T'_π. We show that $T_\pi = T'_\pi$ is always held.

Since the tags are generated by the same user in the same system, the private keys and the public parameters are equal. Therefore, the following equation will be established.

$$Pr[T'_\pi = Be_\pi = T\pi] = 1.$$

□

B. SECURITY ANALYSIS

In this section we will give the security proof of our scheme. In the following proofs, we need three oracles O_K, O_S, and O_H introduced in section 2.

Theorem 3: The proposed scheme is unforgeable under the CF assumption.

Proof: Suppose an adversary C could forge the linkable signature, we will show that there is a polynomial algorithm that can solve the CF problems with non-negligible probability. We will assume there's a simulator S. It can output signatures for a signer even if he knows nothing about the user's private key in the random oracle model.

The simulator S works as following:

Setup

- Choose a $pk_\pi \in L$.
- Make a key generation oracle O_K, obtained the corresponding sk_π.

Hashquery We assume that adversary C can make queries in O_H. H responds with $(d_1, d_2, \ldots, d_w)$. The response of H is stored in list $H - list$ by adversary C.

Sign In this process, adversary C use the result of the Hashquery, do the follows:

1) Let $T_\pi = Be_\pi, u \in F_q^n$ with $w(u) \le t$.
2) Choose $d_{\pi+1} \in F_q^n$.
3) For $i = \pi+1, \pi+2, \ldots, N, 1, \ldots, \pi-1$:
   - Randomly choose $c_i \leftarrow F_q, r_{i1}, r_{i2} \leftarrow F_q^n$ with $w(r_{ij}) \le t, (j = 1, 2)$.
   - Calculate $r_{z,i} = r_{i1} + c_i r_{i2}$.
   - Calculate
   $$t_{i,1} = Ar_{z,i} - d_i PK_i,$$
   $$t_{i,2} = Br_{z,i} - d_i T_\pi.$$
   - Calculate $d_{i+1} = H(L, T_\pi, m, t_{i,1}, t_{i,2})$.
4) Set $d_{\pi+1} \leftarrow H(L, T_\pi, m, Au, Bu)$.
5) Return $(d_1, (r_{z,i}), T_\pi)$.

If the signature can pass the verify algorithm then we consider d_{j+1} is obtained after C makes the *Hashquery*.

Now, we compare the forged signatures with legitimate ones:

$$\begin{aligned} d'_{i+1} &= H(L, T_\pi, m', Ar'_{z,i} - d_i PK_i, Br'_{z,i} - d_i T_\pi) \\ &= H(L, T_\pi, m, Ar_{z,i} - d_i PK_i, Br_{z,i} - d_i T_\pi) \\ &= d_{i+1}. \end{aligned}$$

If

$$\begin{aligned} m &\ne m' \\ Ar'_{z,i} - d_i PK_i &\ne Ar_{z,i} - d_i PK_i \\ Br'_{z,i} - d_i T_\pi &\ne Br_{z,i} - d_i T_\pi \end{aligned}$$

we can find a preimage of d_j.

So, we have

$$\begin{aligned} m &= m' \\ Ar'_{z,i} - d_i PK_i &= Ar_{z,i} - d_i PK_i \\ Br'_{z,i} - d_i T_\pi &= Br'_{z,i} - d_i T_\pi. \end{aligned}$$

That is:

$$A(r'_{z,i} - r_{z,i}) = 0$$
$$B(r'_{z,i} - r_{z,i}) = 0.$$

We assume that $r'_{z,i} \ne r_{z,i}$, so C can find a non-zero vector $s = r'_{z,i} - r_{z,i}$ with $w(r_{z,i}) \le 2t$ such that $As = 0$ and $Bs = 0$. It means that C can solve the CF problem. □

Theorem 4: The proposed scheme is anonymity under the SD assumption.

Proof: Suppose there's a simulator S can be output signatures for a signer l even if he knows nothing about the private key e_l of l.

The simulator S works as below:

Setup Suppose m is the message to be signed and L is the public key list. We use D_t to denote any set of $0 \le t < N$. Choose a $pk_l \in L, \forall sk_i \in D_t, (pk_l, sk_i)$ is not obtained by KeyGen.

Sign In this process, simulator S uses back-patching to generated d_1 and does the follows:

1) Choose a random $e \in F_q^n$ with $w(e) \le t$ and compute $T_l = Be$.
2) Choose $d_1 \in F_q$ uniform randomly.
3) For $i \in \{1, 2, \ldots, N\}$:
   - Randomly selected $c_i \leftarrow F_q, r_{i1}, r_{i2} \leftarrow F_q^n$ with $w(r_{ij}) \le t, (j = 1, 2)$ and calculate $r_{z,i} = r_{i1} + c_i r_{i2}$.
   - Calculate
   $$t_{i,1} = Ar_{z,i} - d_i PK_i,$$
   $$t_{i,2} = Br_{z,i} - d_i T_l.$$
   - Calculate
   $$d_{i+1} = H(L, T_l, m, t_{i,1}, t_{i,2}).$$
4) Set $H(L, T_l, m, t_{N,1}, t_{N,2}) = d_1$.
5) Return $(d_1, (r_{z,i})_{i\in[N]}, T_l)$.

The signature can pass the verify algorithm, then we compare the forged signatures with legitimate ones, we can see:

TABLE 6. Parameter settings and size for our scheme.

Parameter description	1	2	3	4
s	8	32	64	128
n	1268	1268	1268	1268
$k = n/2$	634	634	634	634
t	130	130	130	130
Private key size	634 bits	634 bits	634 bits	634 bits
public key size	1268 bits	1268 bits	1268 bits	1268 bits
Signature ($N = 1$)	$\approx 1.86KB$	$\approx 7.43KB$	$\approx 14.86KB$	$\approx 29.73KB$
Signature ($N = 5$)	$\approx 6.81KB$	$\approx 27.24KB$	$\approx 54.49KB$	$\approx 108.98KB$
Signature ($N = 8$)	$\approx 10.52KB$	$\approx 42.1KB$	$\approx 84.2KB$	$\approx 168.4KB$
Signature ($N = 16$)	$\approx 20.43KB$	$\approx 81.73KB$	$\approx 163.46KB$	$\approx 326.92KB$
Signature ($N = 32$)	$\approx 40.25KB$	$\approx 160.98KB$	$\approx 321.96KB$	$\approx 643.92KB$
Signature ($N = 64$)	$\approx 79.87KB$	$\approx 319.48KB$	$\approx 638.96KB$	$\approx 1277.92KB$
Signature ($N = 128$)	$\approx 159.12KB$	$\approx 636.48KB$	$\approx 1272.96KB$	$\approx 2545.92KB$

$T_l = Be$ where e is chosen random from F_q^n is not obtained from e_l. It means that an adversary cannot distinguish $T_l = Be$ and $T_l = Be_l$.

So, we can find a e such that $T_l = Be$ and the *SD* problem can be solved. □

Theorem 5: Our scheme is linkable under the GSD assumption.

Proof: We assume there's an adversary C and a simulator S. S works as following:

- Setup: Let $A, B \in F_q^{(n-k)\times n}$.
- S can use the KeyGen algorithm to generate the private key e_i and the public key pk_i for the user in the set. When adversary C makes a KeyGen query, S gives a response by the e_π.
- Suppose that adversary C generates two signatures σ, σ' for the message m, m' with the list L, L'. Both signatures can pass the verification algorithm. Then we can obtain:

$$\begin{aligned} dpk_\pi &= Ar_{z,i}, \\ d'pk_\pi &= Ar'_{z,i}, \\ dT &= Br_{z,i}, \\ d'T &= Br'_{z,i}. \end{aligned}$$

Reducing these equations, we can get:

$$\begin{aligned} pk_\pi(d-d') &= A(r_{z,i}-r'_{z,i}), \\ T(d-d') &= B(r_{z,i}-r'_{z,i}). \end{aligned}$$

Sice $pk_\pi = Ae_\pi$, $T = Be_\pi$, we have:

$$\begin{aligned} Ae_\pi(d-d') &= A(r_{z,i}-r'_{z,i}), \\ Be_\pi(d-d') &= B(r_{z,i}-r'_{z,i}). \end{aligned}$$

The following two cases are discussed.

1) If $(d-d') = r_{z,i} - r'_{z,i}$, then

$$T_\pi = Be_\pi = B\frac{r_{z,i}-r'_{z,i}}{[(d-d')]^{-1}} = T.$$

This hypothesis contradicts the tag T is different from all created tags honestly.

2) If $(d-d') \neq (r_{z,i} - r'_{z,i})$, then, we can find a same $s = r_{z,i} - r'_{z,i}$ with $w(s) \leq 2t$ such that

$$\begin{aligned} A' &= A(r_{z,i}-r'_{z,i}), \\ B' &= B(r_{z,i}-r'_{z,i}). \end{aligned}$$

It means that *GSD* problem can be solved. □

The authors in [34] have proved that all linkable ring signature schemes that satisfy unforgeability and linkability are satisfies non slanderability. So, we can claim that our scheme is non-slanderable by theorem 3 and theorem 5.

Theorem 6: Our scheme is non-slanderable under the CF and GSD assumption.

VII. PERFORMANCE ANALYSIS

In this section, we will discuss the parameter selection and the comparison of code-based linkable ring signature.

We consider the parameter selection the same as [13]. $n = 1268$, $k = n/2$, and $t = 130$. Note that, even if knowing $t/2$ positions of the error vector, the code with these parameters still has a security of at least 80 bits.

In our scheme, we set $q = 2^s$, the signature size is related to the value of s and the number of users N. The size of our signature is $(1+(N+1)n-k)s$ bits. Specific analysis is given below.

The signature is $(d_1, (r_{z,i}), T_\pi)$, $i = 1, 2, \ldots, N$.

- For $d_1 \in F_q$, it has s bits.
- For each $r_{z,i}$, it consists of ns bits.
- The size of *Tag* is same as the public key, consists of $(n-k)s$ bits.

This account in total is

$$s + N \times\ nsbits + (n-k)sbits = (1+(N+1)n-k)sbits.$$

For $n = 1268$, $k = 634$, we consider the value of q to be at least 256, that is, s is equal to 8. The parameter settings and size for our scheme is shown in Table 2. We give four different version of our scheme. There versions vary with the value of s.

In terms of performance, our scheme is compared with some existing schemes in the literature [13] as shown in Table 1. It can be show that our scheme is better than these schemes.

VIII. CONCLUSION AND FUTURE WORK

In this study, single-layer and multilayer code-based linkable ring signature schemes based on Borromean ring signature were addressed. They correspond to the case of single input and multiple inputs respectively. Then, we proved the security of proposed schemes under the assumptions of Syndrome Decoding problem, General Syndrome Decoding and Codeword Finding problem. The results showed that our schemes have all the properties that a linkable ring signature scheme should have, i.e., unforgeability, anonymity, linkability and non-slanderability. Efficiency analysis showed that the schemes have smaller signature size than the existing scheme under the same security conditions.

In future, we will consider improving the size of the public key for code-based linkable ring signature. More experimental constructions for linkable ring signature scheme, e.g. hash-based, multivariate-based and lattice-based are also our future work.

REFERENCES

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[3] E. R. Sanseverino, M. L. Di Silvestre, P. Gallo, G. Zizzo, and M. Ippolito, "The blockchain in microgrids for transacting energy and attributing losses," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom) and IEEE Smart Data (SmartData)*, Jun. 2017, pp. 925–930.

[4] G. Suciu, M.-A. Sachian, M. Dobrea, C.-I. Istrate, A. L. Petrache, A. Vulpe, and M. Vochin, "Securing the smart grid: A blockchain-based secure smart energy system," in *Proc. 54th Int. Univ. Power Eng. Conf. (UPEC)*, Sep. 2019, pp. 1–5.

[5] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[6] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2001, pp. 552–565.

[7] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, 2004, pp. 325–335.

[8] S. Noether, "Ring signature confidential transactions for monero," IACR Cryptol. ePrint Archive, Tech. Rep., 2015, p. 1098.

[9] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2017, pp. 456–474.

[10] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2013, pp. 40–56.

[11] Z. Liu, K. Nguyen, G. Yang, H. Wang, and D. S. Wong, "A lattice-based linkable ring signature supporting stealth addresses," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2019, pp. 726–746.

[12] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2002, pp. 415–432.

[13] P. Branco and P. Mateus, "A code-based linkable ring signature scheme," in *Proc. Int. Conf. Provable Secur.* Cham, Switzerland: Springer, 2018, pp. 203–219.

[14] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 157–165, Jan. 2014.

[15] M. H. Au, S. S. Chow, W. Susilo, and P. P. Tsang, "Short linkable ring signatures revisited," in *Proc. Eur. Public Key Infrastruct. Workshop*. Berlin, Germany: Springer, 2006, pp. 101–115.

[16] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Certificate based (linkable) ring signature," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.* Berlin, Germany: Springer, 2007, pp. 79–92.

[17] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, "Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction," *Theor. Comput. Sci.*, vol. 469, pp. 1–14, Jan. 2013.

[18] P. P. Tsang and V. K. Wei, "Short linkable ring signatures for e-voting, e-cash and attestation," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.* Berlin, Germany: Springer, 2005, pp. 48–60.

[19] J. K. Liu and D. S. Wong, "Enhanced security models and a generic construction approach for linkable ring signature," *Int. J. Found. Comput. Sci.*, vol. 17, no. 6, pp. 1403–1422, Dec. 2006.

[20] J. K. Liu and D. S. Wong, "Linkable ring signatures: Security models and new schemes," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin, Germany: Springer, 2005, pp. 614–623.

[21] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity," in *Proc. Int. Conf. Provable Secur.* Berlin, Germany: Springer, 2010, pp. 166–183.

[22] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Efficient linkable and/or threshold ring signature without random oracles," *Comput. J.*, vol. 56, no. 4, pp. 407–421, Apr. 2013.

[23] D. Zheng, X. Li, K. Chen, and J. Li, "Linkable ring signatures from linear feedback shift register," in *Proc. Int. Conf. Embedded Ubiquitous Comput.* Berlin, Germany: Springer, 2007, pp. 716–727.

[24] M. K. Franklin and H. Zhang, "A framework for unique ring signatures," IACR Cryptol. ePrint Archive, 2012, p. 577.

[25] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," in *Proc. Theory Cryptogr. Conf.* Berlin, Germany: Springer, 2006, pp. 60–79.

[26] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2007, pp. 181–200.

[27] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad hoc groups," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2004, pp. 609–626.

[28] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *IJ Netw. Secur.*, vol. 5, no. 2, pp. 154–157, 2007.

[29] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Proc. IMA Int. Conf. Cryptogr. Coding*. Berlin, Germany: Springer, 2009, pp. 222–235.

[30] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4833–4842, Jul. 2011.

[31] A. Petzoldt, S. Bulygin, and J. Buchmann, "A multivariate based threshold ring signature scheme," *Applicable Algebra Eng., Commun. Comput.*, vol. 24, nos. 3–4, pp. 255–275, Aug. 2013.

[32] C. Aguilar-Melchor, S. Bettaieb, P. Gaborit, and J. Schrek, "A code-based undeniable signature scheme," in *Proc. IMA Int. Conf. Cryptogr. Coding*. Berlin, Germany: Springer, 2013, pp. 99–119.

[33] E. Berlekamp, R. Mceliece, and H. Van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 384–386, May 1978.

[34] W. A. A. Torres, R. Steinfeld, A. Sakzad, J. K. Liu, V. Kuchta, N. Bhattacharjee, M. H. Au, and J. Cheng, "Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1.0)," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Cham, Switzerland: Springer, 2018, pp. 558–576.

[35] C. Baum, H. Lin, and S. Oechsner, "Towards practical lattice-based one-time linkable ring signatures," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2018, pp. 303–322.

YAN REN received the bachelor's degree from Shanxi Normal University, Linfen, China, in 2004, the master's degree from Shaanxi Normal University, Xi'an, China, in 2010, and the Ph.D. degree from Guangzhou University, Guangzhou, China, in 2014. Her primary research interests are applied cryptography, in particular, cryptographic protocols, encryption and signature schemes, and anonymous systems. She has published some interesting results of signature schemes.

QIUXIA ZHAO received the B.Eng. and M.Eng. degrees from Yunnan University, Kunming, China, in 2009 and 2012, respectively. She is currently a Teaching Assistant with Yuncheng University. Her research interests include data science and information security.

HAIPENG GUAN received the M.Eng. degree from Hunan Normal University, Changsha, in 2006, and the M.Eng. degree from South China Normal University, in 2009. She is currently a Lecturer with Yuncheng University. Her research interests include data science and information security.

ZHIQIANG LIN received the B.Eng. and M.Eng. degrees from South China Normal University, Guangzhou, China, in 2007 and 2010, respectively, and the Ph.D. degree from Guangzhou University, Guangzhou, in 2014. He was a Postdoctoral Researcher with the Institute of Information Engineering, Chinese Academy of Sciences, China, from 2014 to 2016. He is currently a Lecturer with Guangzhou University. His research interests include distributed parameter system control and cryptology.