An Identity based Linkable Ring Signature with Logarithmic Size

Mohamed Nassurdine[1,3], Huang Zhang[2], and Fangguo Zhang[1,3,⋆]

[1] School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510006, China

[2] School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China

[3] Guangdong Key Laboratory of Information Security Technology, Guangzhou 510006, China

Abstract. Anonymity is an inevitable and sensitive matter of concern, especially in the age where people are willing to use digital devices and Internet to deal with almost all things in their work and daily life. To support anonymity, modern cryptography is one of the most suitable choices in the algorithm level. Particularly, in the scenarios, such as e-voting, crypto-currency, and smart grid *etc*, a cryptographic primitive, called linkable ring signature, has shown its ability to handle anonymity problems. However, signature schemes will introduce additional costs to those e-commerce systems, so that they should be as efficient as possible. On the other side, a signature scheme that requires the public key infrastructure (PKI) brings much unnecessary inconvenience to its users, since typically, users of the aforementioned systems are not familiar with cryptographic skills and the system establishers are trusted by them in some sense. As a result, an identity-based (ID-based) signature scheme with small size fulfills the visible requirements of e-commerce systems. In this paper, we proposed an ID-based linkable ring signature scheme with logarithmic size from paring and elliptic curve discrete logarithm problem (ECDLP), and gave all the security proofs in detail. Besides that, the scheme needs no trusted setup, except that the key generation center knows the secret key of each user and it is a property of ID-based cryptography in nature. As far as we know, our scheme is the best result in this area to date.

Keywords: Anonymity; ID-based Linkable ring signature; Logarithmic size; Paring

⋆ Corresponding author, `isszhfg@mail.sysu.edu.cn`

1 Introduction

Linkable ring signature, as a variant of ring signature [26], has been studied for many years [22]. It is significantly useful in several e-commerce systems, such as e-voting, smart grid, *etc.* In recent years, linkable ring signatures receives a lot of attentions, due to the fast development of blockchain-based crypto-currencies. Researchers suggest to use such a signature to handle anonymity problems and keep the block-chain system lightweight [27]. Informally speaking, (linkable) ring signatures grants a system the ability to anonymously authenticate their users, while keep the costs at a low level. Comparing to a system that employs general purpose zero-knowledge proof protocols to support anonymity [28], a (linkable) ring signature based one is typically more efficient. Consequently, efficiency is an important index to measure the performance of a (linkable) ring signature, and a small signature size would be a desirable property for such a scheme. On the other side, as linkable ring signatures are very suitable for e-commerce systems, and such a system is efficiency sensitive, it is nature to consider that the association between a standard signature scheme and the PKI would bring much unnecessary inconvenience. For instance, sometime the group of an e-voting event is organized temporary so that to get a certificate from the PKI is a boring work for group members to do. As for smart grid, such a system is typically established by an authority party, and thus users delivers enough trusts to the system holder in some sense. Since ID-based cryptography is one of the directions to avoid the PKI [8], it is nature for us to equip our linkable ring signature with an ID-based property. That will make an e-commerce system more flexible to deploy a cryptographic scheme for security consideration.

Now, we have a common sense on that a (linkable) ring signature scheme in e-commerce system should be efficient and convenient. However, generally speaking, a traditional (linkable) ring signature usually features a signature size of $O(n)$, where n is the cardinality of the ring. A more satisfactory result would be $O(\log n)$ or $O(1)$, which means the signature size is slightly influenced by or independent of the number of participants. The first ID-based ring signature is in [30], and several works appears since then [4,13]. They were all proved in the random oracle model, and the signature size is linear in the cardinality of the ring. Only a few works were constructed in the standard model [3, 6, 12], but at least their signature size is not desirable enough, except those in [5, 10, 18, 20]. Fortunately, by using accumulator, constant size (ID-based linkable) ring signatures could be designed

[1, 2, 11, 14, 24, 29]. When considering no trusted setup, there are two original $O(\log n)$ ring signatures based on number-theoretic assumptions [9, 17], and the logarithmic-size ring signatures with Tight Security [19]. Currently, some elegant short ring signature schemes were proposed relying on various assumptions [7, 23]. However, neither of them is ID-based or contains the property of linking. To fill a vacancy in this area, in this paper, we design an ID-based linkable ring signature with logarithmic size, by using the strategies from [17] and parings. Amounts of proof skills are inspired by their work, so that if readers are familiar with the framework of [17], they can better understand the construction and proofs in the current paper.

In the literature [17], Groth *et al.* designed a ring signature with logarithmic size, but in fact, this signature scheme is a Fiat-Shamir transformation of a Sigma-protocol for one-out-many-proofs. An underlying cryptographic primitive is a homomorphic commitment scheme, such as the Pedersen commitment in DLP (Discrete Logarithm Problem) settings. To finish their one-out-of-many proofs, they also introduced a Sigma-protocol for proving in zero knowledge that such a commitment is opened to 1 or 0. Our major work is to improve the ECDLP-based version of that in [31] to an ID-based one, and because of the new problems brought by the modifications, we redesigned the corresponding security proofs, so that the scheme could convince users that it is unforgeable under the adaptively chosen message and ID attack in the random oracle model and so on.

The remaining of this paper is organized as follows: in Sect. 2 we introduce notations and concepts used in this work. The details of the construction and the security proofs are described in Sect. 3. Finally, we give a short conclusion and further consideration in Sect. 4.

2 Preliminaries

This section gives a brief introduction to the notations, definitions adopted in this paper.

2.1 Notations

We use $\mathbb{Z}$, $\mathbb{N}$ to denote the set of all integers, and the set natural numbers. If $a, b \in \mathbb{Z}$ and $a < b$, then $[a, b]$ is the set $\{x \in \mathbb{Z} : a \leq x \leq b\}$ and $[a, b)$ is the set $\{x \in \mathbb{Z} : a \leq x < b\}$. For an integer i, i_j symbolizes the j-th bit of i. $\delta_{i\ell}$

is Kronecker's delta, *i.e.*, $\delta_{\ell\ell} = 1$ and $\delta_{i\ell} = 0$ for $i \neq \ell$. A set $\{x_1, \ldots, x_n\}$ will be denoted by $\{x_i\}_{i=1}^n$ for short. We use $|S|$ to indicate the cardinality of a set finite S, and $a \leftarrow S$ means a is chosen from S uniformly at random. We use the standard big O notation and write $\mathrm{negl}(n)$ as a negligible function (probability) and $1 - \mathrm{negl}(n)$ is called overwhelming probability.

2.2 Bilinear maps

Definition 1. *Let $\mathbb{G} = \langle G \rangle$, $\mathbb{G}_T$ be two (additive) cyclic groups of prime order p. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a paring if it is satisfies the following properties.*

- Bilinear*: For any $x, y \in \mathbb{Z}_p$, we have $e(xG, yG) = xy \cdot (G, G)$.*
- Non-degenerate*: If $P, Q \in \mathbb{G}$ are two generators of $\mathbb{G}$, then $e(P, Q)$ generates G_T.*
- Computability*: There is an efficient algorithm to compute $e(P, Q)$, for all $P, Q \in \mathbb{G}$.*

2.3 Pedersen Commitment

Pedersen commitment [25] allows a user to construct a commitment to a value and any party could check whether the value opened later is the one which was committed at the beginning. The scheme involves a pair of efficient algorithms $(\mathbf{Gen}, \mathbf{Com})$

- $\mathbf{Gen}(1^\lambda)$: On input a security parameter λ, the algorithm generates a cyclic group $\mathbb{G}$ of prime order p. It then selects two generators. Finally, $G, H \in \mathbb{G}$ at random. $\{\mathbb{G}, p, G, H\}$ will be published as the public parameters.
- $\mathbf{Com}(x, y)$: On input a value $x \in \mathbb{Z}_p$, and a randomly chosen $y \leftarrow \mathbb{Z}_p$, this algorithm computes and outputs a commitment $c = xH + yG$. The commitment c can later be opened by giving x, y.

Pedersen commitment is perfect hiding and is computational biding if the DLP corresponding to $\mathbb{G}$ is hard.

2.4 ID-based Linkable Ring Signature

The following definition of an ID-based linkable ring signature comes from [1]. Such a signature scheme consists of five efficient algorithms (**Setup**, **Ext**, **Sign**, **Vfy**, **Link**).

- $pp \leftarrow \mathbf{Setup}(1^\lambda)$: On input a security parameter λ, the algorithm outputs a master secret key v and a list of system parameters pp that includes λ and the descriptions of a user secret key space $\mathcal{D}$, a message space $\mathcal{M}$, an event-id space $\mathcal{EID}$ as well as a signature space Ψ.
- $V_i \leftarrow \mathbf{Ext}(\mathrm{ID}_i, v)$: On input an identity $\mathrm{ID}_i \in \{0,1\}^*$ for a user and the master secret key v, this algorithm outputs the user's secret key $V_i \in \mathcal{D}$. This algorithm is usually executed by a trusted party called Private Key Generator (PKG).
- $\sigma \leftarrow \mathbf{Sign}(V_j, \mathrm{msg}, event, L)$: On input a group size n of length polynomial in λ, a set $L = (\mathrm{ID}_i)_{i=1}^n$ of n user identities, a message $\mathrm{msg} \in \mathcal{M}$, an event-id $event \in \mathcal{EID}$, and a secret key $V_j, j \in [n]$, the algorithm outputs an ID-based linkable ring signature $\sigma \in \Psi$.
- $\{0,1\} \leftarrow \mathbf{Vfy}(\mathrm{msg}, event, L, \sigma)$: Verify a purported signature σ on a message msg with respect to the ring L and the event-id $event$. The algorithm outputs 1 if it accepts the signature and outputs 0 otherwise.
- $\{0,1\} \leftarrow \mathbf{Link}(event, \mathrm{msg}_1, L_1, \sigma_1, \mathrm{msg}_2, L_2, \sigma_2)$: On input two accepting signatures σ_1, σ_2 on the same event-id $event$, output 1 if the signatures are linked, and output 0 otherwise.

A linkable ring signature is cryptographically useful, only if it is correct and secure. The definitions for correctness and security come from a combination of [1] and [21]. Correctness states that signatures signed according to the scheme should be accepted during verification.

Definition 2 (Perfect correctness). *An ID-based linkable ring signature scheme is of perfect correctness, if for any* $pp \leftarrow \mathbf{Setup}(1^\lambda)$, $\mathrm{ID} \in \{0,1\}^*$, $V \leftarrow \mathbf{Ext}(\mathrm{ID}, v)$, *any* L *such that* $\mathrm{ID} \in L$, $event \leftarrow \mathcal{EID}$, $\mathrm{msg} \leftarrow \mathcal{M}$, *and* $\sigma \leftarrow \mathbf{Sign}(V, \mathrm{msg}, event, L)$.

$$\Pr[\mathbf{Vfy}(\mathrm{msg}, event, L, \sigma) = 1] = 1 \ .$$

Security of linkable ring signature schemes involves unforgeability, anonymity, linkability, and nonslanderbility which will be defined as follows. All of them are defined by a game between a Simulator $\mathcal{S}$ (usually acted by a challenger $\mathcal{C}$) and a PPT adversary $\mathcal{A}$. The following three kinds of oracles below are crucial in the description of security proofs.

- $V_i \leftarrow \mathcal{EO}(\mathrm{ID}_i)$: The stateful *Extraction Oracle*, on input ID_i, returns the corresponding secret key V_i.

- $\sigma \leftarrow \mathcal{SO}(\mathrm{ID}_i, \mathrm{msg}, event, L)$: The *Signing Oracle*, on input $event \in \mathcal{EID}$, a ring L, an identity $\mathrm{ID}_i \in L$, and a message $\mathrm{msg} \in \mathcal{M}$, returns a valid signature σ.
- $\mathbf{y} \leftarrow \mathcal{RO}(\mathbf{x})$: If the scheme is proven in the random oracle model, hash functions are modeled as random oracles. On input an element from the domain of the random oracle, returns the corresponding element in the range.

Unforgeability ensures that an adversary could not forge any signature just from the identities of the ring, even though during the forging attack, it can obtain message-signature pairs and the target ring is chosen by itself.

The unforgeability game is defined as follows:

1. A simulator $\mathcal{S}$ takes a sufficiently large security parameter λ and runs **Setup** to generate the public parameters pp and master secret key s. The adversary $\mathcal{A}$ is given pp.
2. $\mathcal{A}$ can make a polynomial number of oracle queries to $\mathcal{EO}$, $\mathcal{SO}$ and $\mathcal{RO}$ adaptively.
3. $\mathcal{A}$ outputs a signature σ^* for message m^* and ring L^*.

$\mathcal{A}$ wins the above game if

- $\mathbf{Vfy}(\mathrm{msg}, event, L^*, \sigma^*) = 1$;
- (L^*, m^*) and σ^* should not be in the set of oracle queries and replies between $\mathcal{A}$ and $\mathcal{SO}$; and
- $\mathcal{A}$ did not query $\mathcal{EO}$ on any identity $\mathrm{ID} \in L^*$.

Denote the advantage of $\mathcal{A}$ in winning this game by

$$\mathbf{Adv}_{\mathcal{A}}^{Forge}(\lambda) = \Pr[\mathcal{A} \text{ wins the game}] \ .$$

Definition 3 (Unforgeability). *An ID-based linkable ring signature scheme is unforgeable under the adaptively chosen message and ID attack if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{forge}(\lambda)$ is negligible.*

Weak anonymity requires that any party cannot know the actual signer of a ring signature, if all of the parties of the ring do not reveal their identity. Such a property is defined in the following game *Anon* between the Simulator $\mathcal{S}$ and the PPT adversary $\mathcal{A}$

- $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters pp.

- $\mathcal{A}$ may query $\mathcal{EO}$, $\mathcal{SO}$, and $\mathcal{RO}$ with arbitrary strategies.
- $\mathcal{A}$ gives $\mathcal{S}$ an event-id $event \in \mathcal{EID}$, a message $\mathrm{msg} \in \mathcal{M}$, and a ring L such that all of the identities were not submitted to $\mathcal{EO}$.
- $\mathcal{S}$ randomly picks $i \in [1, |L|]$ and computes $\sigma_i = \mathbf{Sign}(V_i, \mathrm{msg}, event, L)$, where V_i is the corresponding secret key of ID_i. σ_i is given to $\mathcal{A}$.
- $\mathcal{A}$ outputs a guess $i' \in [1, |L|]$.

We denote $\mathcal{A}$'s advantage in winning this game by

$$\mathbf{Adv}_{\mathcal{A}}^{Anon}(\lambda) = \left| \Pr[i' = i] - \frac{1}{|L|} \right| .$$

Definition 4 (Anonymity). *A linkable ring signature scheme is of weak anonymity if for any PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{Anon}(\lambda) = \mathrm{negl}(\lambda)$.*

Linkability requires that if less tan two user private keys are known, then no adversary could generate two valid signatures on the same event-id such that these signatures are not linked. Such a property is defined by the following game between Simulator $\mathcal{S}$ and the PPT adversary $\mathcal{A}$.

1. $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters pp.
2. $\mathcal{A}$ may query the oracles according to any adaptive strategy.
3. $\mathcal{A}$ gives $\mathcal{S}$ an event-id $event \in \mathcal{EID}$, two rings L_1 and L_2, two messages $\mathrm{msg}_1, \mathrm{msg}_2 \in \mathcal{M}$, and the corresponding signatures $\sigma_1, \sigma_2 \in \Psi$.

$\mathcal{A}$ wins the game if

- $\mathbf{Vfy}(\mathrm{msg}_i, event, L_i, \sigma_i) = 1$ for $i = 1, 2$ such that σ_i are not outputs of $\mathcal{SO}$;
- $\mathcal{EO}$ has been queried less than two times; and
- $\mathbf{Link}(\sigma_1, \sigma_2) = 0$.

The advantage of $\mathcal{A}$ in winning this game is denoted by $\mathbf{Adv}_{\mathcal{A}}^{Link}(\lambda) = \Pr[\mathcal{A} \text{ wins the game}]$.

Definition 5 (Linkability). *An ID-based linkable ring signature scheme is linkable if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{Link}(\lambda)$ is negligible.*

Nonslanderability ensures that no signer can generate a signature which is determined to be linked with another signature which is not generated by the signer. It is defined in the following game between the simulator $\mathcal{S}$ and the adversary $\mathcal{A}$ in which $\mathcal{A}$ is given access to oracles $\mathcal{EO}$, $\mathcal{SO}$ and the random oracle.

1. $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters pp.

2. A may query the oracles according to any adaptive strategy.
3. A gives $\mathcal{S}$ an event-id *event*, a message msg, a ring L, the identity of an insider ID_π such that it has not been queried to $\mathcal{EO}$ or has not been included as the insider identity of any query to $\mathcal{SO}$. $\mathcal{S}$ uses the private key V_π corresponding to ID_π to run $\mathbf{Sign}(V_j, \mathrm{msg}, event, L)$ and to produce a signature σ' given to $\mathcal{A}$.
4. $\mathcal{A}$ queries oracles with arbitrary interleaving. Except ID_π cannot be queries to $\mathcal{EO}$, or included as the insider identity of any query to $\mathcal{SO}$. In particular, A is allowed to query any identity that is not ID_π to $\mathcal{CO}$.
5. $\mathcal{A}$ deliver a ring L^*, a message msg^*, and a signature $\sigma^* \neq \sigma$.

$\mathcal{A}$ wins the game if

- $\mathbf{Vfy}(\mathrm{msg}, event, L, \sigma) = 1$;
- σ^* is not an output of $\mathcal{SO}$;
- ID_π has not been queried to $\mathcal{CO}$; and
- $\mathrm{Link}(event, \mathrm{msg}, L, \sigma, \mathrm{msg}^*, L^*, \sigma^*) = 1$.

Denote the advantage of $\mathcal{A}$ in winning this game by $\mathbf{Adv}_{\mathcal{A}}^{NS}(\lambda) = \Pr[\mathcal{A}$ wins the game$]$.

Definition 6 (Nonslanderability). *An ID-based linkable ring signature scheme is nonslanderable if for all PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{NS}$ is negligible.*

3 ID-based Linkable Ring Signature Scheme

In this section, we introduce the construction of the signature scheme and also the details of its security proofs. Since the framework of the construction is inspired by the spirits of [17], actually, the signature scheme is a Fiat-Shamir transformation [15] version of a public coin 3-move interactive argument of knowledge system which is also known as a Sigma-protocol [16]. Since the protocol and the signature scheme involves a lot of duplicative parts, we put its description and security proofs in the App. B. Note that, since the protocol was built based on the ECDLP, it could be set up in the common random string model.

3.1 The Construction

Before giving the main body of the construction, a technique adopted in [17] should be stated. The following parameters are the same as that in our construction.

Since we could duplicate some ring members, we could let n be the size of the ring and $m = \log n$ be an integer. Define $f_{j,1} = f_j = \ell_j x + a_j = \delta_{1\ell_j} x + a_j$, and $f_{j,0} = x - f_j = (1 - \ell_j)x - a_j = \delta_{0\ell_j} x - a_j$. For every $i \in [0, n)$ the product $\prod_{j=1}^{m} f_{j,i_j}$ is a polynomial in the indeterminate x of the form

$$p_i(x) = \prod_{j=1}^{m} (\delta_{i_j \ell_j} x) + \sum_{k=0}^{m-1} p_{i,k} x^k = \delta_{i\ell} x^m + \sum_{k=0}^{m-1} p_{i,k} x^k.$$

Here, $p_{i,k}$ is the coefficient of the kth degree term of the polynomial $p_i(x)$, and can be efficiently computed when $\{a_j\}_{j=1}^{m}$, i and ℓ are given.

The linkable ring signature based on ECDLP consists of five efficient procedures (**Setup**, **Ext**, **Sign**, **Vfy**, **Link**).

Setup(1^λ): The input of this procedure is a security parameter λ. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Let $G \in E$ be a point of prime order p, here $\log p = O(\lambda)$ and let $\mathbb{G}$ be the prime order subgroup of E generated by G. Choose another element $H \in \mathbb{G}$ randomly. Let $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$, $\mathcal{H}_1 : \{0,1\}^* \to \mathbb{G}$, $\mathcal{H}_2 : \{0,1\}^* \to \mathbb{G}$, be three cryptographic hash functions, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ a paring. Select a master secret key $v \leftarrow \mathbb{Z}_p^*$ and compute the master public key $P = vG$. The output of this procedure is $pp = (\mathbb{G}, G, H, P, p, q, \mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, e)$ and it is an implicit input for the other procedures.

Ext(ID, Q, v): Given an identity $\mathrm{ID} \in \{0,1\}^*$ and its corresponding public key Q, the algorithm first check whether $\mathcal{H}_1(\mathrm{ID}) = Q$. If yes, it computes the associated secret key $V = vQ$.

Sign$(L, V_\ell, \mu, event)$: Let $L = (Q_0, \ldots, Q_{n-1})$ be the ensemble of a ring and $m = \log n$. On input a message μ, the ℓth identity's signature on behalf of L in the event description *event* is generated as follows

- compute $K = \mathcal{H}_2(event)$, $I = e(V_\ell, K)$,
- For j from 1 to m,
  - choose $r_j, a_j, s_j, t_j \leftarrow \mathbb{Z}_p$ uniformly at random,
  - compute $A_j = \ell_j H + r_j G$,
  - compute $B_j = a_j H + s_j G$,
  - compute $C_j = a_j \ell_j H + t_j G$.
- For k from 0 to $m - 1$,
  - choose $\rho_k \leftarrow \mathbb{Z}_p$ uniformly at random,
  - compute $D_k = (\sum_{i=0}^{n-1} p_{i,k} Q_i) + \rho_k G$,
  - compute $E_k = e(P, \rho_k K)$.

- Let $\mathbf{a} = \{A_j, B_j, C_j, D_{j-1}E_{j-1}\}_{j=1}^m$ and compute $x = \mathcal{H}(\mu, L, \mathbf{a}, I, event)$.
- For j from 1 to m, compute
  - $w_j = x\ell_j + a_j \bmod p$,
  - $y_j = xr_j + s_j \bmod p$,
  - $z_j = (x - w_j)r_j + t_j \bmod p$.
- $Z = x^m V_\ell - \sum_{k=0}^{m-1} \rho_k x^k P \bmod p$.
- Let $\mathbf{b} = \{w_j, y_j, z_j\}_{j=1}^m$. Publish $\sigma = \{\mathbf{a}, x, \mathbf{b}, Z, I\}$ as the signature of u with respect to L and $event$.

$\mathbf{Vfy}(\mu, L, event, \sigma)$:

- Check if $x = \mathcal{H}(\mu, L, \mathbf{a})$. Return 0 and abort if it is not
- Compute $K = \mathcal{H}_2(event)$
- For j from 1 to m, consider the following equalities
  - $xA_j + B_j = w_j H + y_j G$,
  - $(x - w_j)A_j + C_j = z_j G$.

  If any of them doesn't hold, output 0 and abort.
- Inspect whether $x^m I - \sum_{k=0}^{m-1} x^k E_k = e(Z, K)$.
- Inspect whether $e\,(Z, G) = e\left(\sum_{i=0}^{n-1}(\prod_{j=1}^m w_{j,i_j})Q_i + \sum_{k=0}^{m-1}(-x^k)D_k, P\right)$.

  If they are not the cases, output 0 and abort; otherwise output 1.

According to the description, an honestly generated signature will always pass the verification.

Theorem 1. *The ID-based linkable ring signature is of perfect correctness.*

Since the result is direct from a simple deduction, we left the proof in App. A.

3.2 Security Proofs

In the proofs, the parameters $\mathbf{a} = \{A_j, B_j, C_j, D_{j-1}E_{j-1}\}_{j=1}^m$, and $\mathbf{b} = \{w_j, y_j, z_j\}_{j=1}^m$ in the scheme will be referred to as *cmt* (Initial message) and *rsp* (Response), respectively.

Theorem 2. *The ID-based linkable ring signature is of weak anonymity in the random oracle model, if the bilinear decisional Diffie-Hellman problem (BDDHP) is intractably solvable.*

Proof. Suppose that $\mathcal{A}$ is a PPT adversary which on input a message m, a ring of n members, a fresh event description *event*, and a valid signature σ on L and m, output with probability great than ϵ the index of the real signer who generated σ. The remaining of the proof is a construction of a PPT challenger (or distinguisher) $\mathcal{C}$ for solving the BDDHP.

Let $\mathbb{G} = \langle G \rangle$ be a cyclic group of prime order p, and $T_1 = (G, aG, bG, cG, w \cdot e(G, G))$, $T_2 = (G, aG, bG, cG, abc \cdot e(G, G))$, where $a, b, c, w \leftarrow \mathbb{Z}_p$ Formally, the BDDHP assumption states that for any PPT distinguisher $\mathcal{C}$,

$$|\Pr[\mathcal{C}(T_1) = 1] - \Pr[\mathcal{C}(T_2) = 1]| \leq \mathrm{negl}(\lambda) \ .$$

When our distinguisher $\mathcal{C}$ is given T_s as input for $s \in \{0, 1\}$, it does as follows to simulate a anonymity game to play with $\mathcal{A}$. For simplicity, we use T_{si} to denote the i-th component of T_s

The challenger $\mathcal{C}$ first provide the public system parameter to the adversary $\mathcal{A}$. To this end, $\mathcal{C}$ directly uses the group description $(\mathbb{G}, G, p, q)$ of the BDDHP. Then it selects $H \leftarrow \mathbb{G}$, and set the master public key $P = T_{s2}$. Finally, $pp = (\mathbb{G}, G, P, p, q, \mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, e)$ will be published, where the hash functions are modeled as random oracles.

Before invoking $\mathcal{A}$, the challenger $\mathcal{C}$ generates a target signature for $\mathcal{A}$ in advance.

- Randomly selects the cardinality of the ring n, n identities $(\mathrm{ID}_i)_{i=0}^{n-1}$, an event description *event*, and a message μ.
- Select $\pi \leftarrow [0, n)$. The public key of the π-th participant is set to be $Q_\pi = T_{s3}$, and the random oracle is modeled to have $\mathcal{H}_1(\mathrm{ID}_\pi) = Q_\pi$.
- For $i \in [1, n) \backslash \{\pi\}$, randomly pick $Q_i \leftarrow \mathbb{G}$, and model the random oracle to have $\mathcal{H}_1(\mathrm{ID}_i) = Q_i$. Let the ring be $L = (Q_0, \ldots, Q_{n-1})$.
- Set the linking tag $I_s = T_{s5}$ and model the random oracle to have $\mathcal{H}_2(event) = T_{s4}$.
- The challenger $\mathcal{C}$ then selects a challenge $x \leftarrow \mathbb{Z}_p$, and use the SHVZK simulator (see App. B) to generate a valid proof transcript $\sigma = (cmt, x, rsp, I_b)$, which is later used as the target signature. After this, $\mathcal{C}$ models the random oracle to have $\mathcal{H}(\mu, L, cmt, I_s, event) = x$.

Subsequently, $\mathcal{C}$ invokes $\mathcal{A}$ with pubic system parameter pp, message μ, ring L, event description *event*, linking tag I_s, and the target signature σ. $\mathcal{A}$ has the

right to oracle access to the extracting oracle, the signing oracle, and the random oracles. $\mathcal{C}$ simulates these oracles as follows.

Random oracle $\mathcal{H}(s)$: if $\mathcal{H}(s)$ was queried before, return the recorded element. Else, the challenger randomly picks and returns $t \leftarrow \mathbb{Z}_p$. Finally it models the random oracle to have $\mathcal{H}(s) = t$.

Random oracle $\mathcal{H}_1(\mathrm{ID})$: if $\mathcal{H}_1(\mathrm{ID})$ was queried before, return the recorded element. Otherwise, $\mathcal{C}$ randomly picks $\alpha \leftarrow \mathbb{Z}_p$ and computes $Q = \alpha G$. Thus, $V = \alpha P$ is the corresponding secret key. The random oracle is modeled to have $\mathcal{H}_1(\mathrm{ID}) = Q$.

Random oracle $\mathcal{H}_2(event)$: if $\mathcal{H}_2(event)$ was queried before, return the recorded element. Otherwise, randomly select $K \leftarrow \mathbb{G}$ and model the random oracle to have $\mathcal{H}_2(event) = K$.

Extracting oracle $\mathcal{EO}(\mathrm{ID}, Q)$: if $\mathcal{H}_1(\mathrm{ID}) = Q$ and $Q \notin L$, the challenger returns $V = \alpha P$. Otherwise, $\mathcal{C}$ refuses to answer.

Signing oracle $\mathcal{SO}(L', Q, \mu, event')$: if there is a public key in L' obtained not from querying $\mathcal{H}_1$ or $Q \notin L'$, the challenger refuses to answer. Else if $Q \notin L$, the challenger runs $\mathbf{Sign}(L, V = \alpha P, \mu, event)$ to generate an accepting signature. Else if $Q \in L$ and $event' \neq event$, the challenger $\mathcal{C}$ uses the SHVZK simulator to generate an accepting signature. Otherwise, $\mathcal{C}$ refuses to answer.

Finally, $\mathcal{A}$ returns an index $j \in [0, n)$. If $j = \pi$, $\mathcal{C}$ outputs 1, otherwise $\mathcal{C}$ outputs 0.

If $\mathcal{C}$ is fed with T_1, then $\mathcal{A}$ is in a real anonymity game with respect to the linkable ring signature. According to the hypothesis to $\mathcal{A}$, we have

$$\Pr[\mathcal{C}(T_1) = 1] = \Pr[\mathcal{A}(params, \mu, L, event, I_1, \sigma) = \pi] \geq \epsilon.$$

On the other side, if $\mathcal{C}$ is fed with T_2, then the advantage for $\mathcal{A}$ to find the correct π is no better than random guessing, since the underlying Sigma-protocol is SHVZK (see App. B) and the linking tag I_2 is independent of every pubic key in L. Thus,

$$\Pr[\mathcal{C}(T_2) = 1] = \Pr[\mathcal{A}(params, \mu, L, event, I_2, \sigma) = \pi] = 1/n.$$

Consequently, depending on the BDDHP assumption

$$\begin{aligned}
\mathrm{negl}(\lambda) &\geq |\Pr[\mathcal{C}(T_1) = 1] - \Pr[\mathcal{C}(T_2) = 1]| \\
&= |\Pr[\mathcal{A}(params, \mu, L, event, I_1, \sigma) = \pi] - \Pr[\mathcal{A}(params, \mu, L, event, I_2, \sigma) = \pi]| \\
&= |\Pr[\mathcal{A}(params, \mu, L, event, I_1, \sigma) = \pi]| - |\Pr[\mathcal{A}(params, \mu, L, event, I_2, \sigma) = \pi]| \\
&\geq \epsilon - 1/n \ .
\end{aligned}$$

Thus we have $\epsilon \leq 1/n + \text{negl}(\lambda)$, which means the advantage for $\mathcal{A}$ to break the weak anonymity of our scheme is negligible. $\square$

Theorem 3. *The ID-based linkable ring signature is unforgeable on adaptively chosen message and ID attacks in the random oracle model, if the Computational Diffie-Hellman problem (CDHP) is intractable to solve.*

Proof. An instance of the CDHP is a tuple $T = (G, aG, bG)$, where G is a generator of the group $\mathbb{G}$ of order p, and $a, b \leftarrow \mathbb{Z}_p$. The goal of this problem is to compute abG. Formally, the CDHP assumption states that for any PPT algorithm (or challenger) $\mathcal{C}$,

$$\Pr[abG \leftarrow \mathcal{C}(T)] \leq \text{negl}(\lambda) \ .$$

On receiving an instance of CDHP $T = (G, T_1, T_2) = (G, aG, bG)$, the challenger $\mathcal{C}$ works as follows to simulate an unforgeability game for $\mathcal{A}$.

The challenger $\mathcal{C}$ first provides the public system parameter to a PPT adversary $\mathcal{A}$ which is supposed to forge an accepting signature with non-negligible probability. To this end, $\mathcal{C}$ directly uses the group description $(\mathbb{G}, G, p, q)$ of the CDHP. Then it selects $H \leftarrow \mathbb{G}$, and set the master public key $P = T_1$. Finally, $pp = (\mathbb{G}, G, P, p, q, \mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, e)$ will be published, where the hash functions are modeled as random oracles.

Random oracle $\mathcal{H}(s)$: the random oracle is simulated the same as in the proof of Theorem 2.

Random oracle $\mathcal{H}_1(\text{ID})$: Let q_v be the maximum number of queries that will be made to the random oracle $\mathcal{H}_1$. The challenger $\mathcal{C}$ randomly picks an index $t \in [1, q_v]$. If ID is the t-th fresh query made by $\mathcal{A}$ (labeled by ID_t), return $\mathcal{H}_1(\text{ID}_t) = Q_t = T_2$ and model the random oracle to have this map. Otherwise, $\mathcal{C}$ checks whether $\mathcal{H}_1(\text{ID})$ has been queried before. If it is not, $\mathcal{C}$ randomly picks $\alpha \leftarrow \mathbb{Z}_p$ and computes $Q = \alpha G$. The random oracle is modeled to have $\mathcal{H}_1(\text{ID}) = Q$. Notice that $V = \alpha P$ is the corresponding secret key.

Random oracle $\mathcal{H}_2(event)$: if $\mathcal{H}_2(event)$ was queried before, return the recorded element. Otherwise, randomly select $\beta \leftarrow \mathbb{Z}_p$ and compute $K = \beta G$. The random oracle is modeled to have $\mathcal{H}_2(event) = K$.

Extracting oracle $\mathcal{EO}(\text{ID}, Q)$: If $Q = Q_t$, abort. If $\mathcal{H}_1(\text{ID}) = Q$, the challenger returns $V = \alpha P$, where $\alpha \leftarrow \mathbb{Z}_p$.

Signing oracle $\mathcal{SO}(L, Q, \mu, event)$: if there is a public key in L obtained not from querying $\mathcal{H}_1$ or $Q \notin L$, the challenger refuses to answer. Else if $Q \neq Q_t$,

the challenger runs $\mathbf{Sign}(L, V = \alpha P, \mu, event)$ to generate an accepting signature. Else if $Q = Q_t$, the challenger $\mathcal{C}$ sets the linking tag to be $I = e(Q, \beta P)$ and uses the SHVZK simulator to generate an accepting signature. Otherwise, $\mathcal{C}$ refuses to answer.

Finally, $\mathcal{A}$ will return a signature σ^* on L^*, μ^*, $event^*$ with non-negligible probability, such that the public keys in L was not submitted to $\mathcal{EO}$ and σ^* was not generated by $\mathcal{SO}$.

According to the analysis in Theorem 4 of [17], $\mathcal{C}$ is able to obtain $n+1$ distinct challenge-response pairs to the same initial message, so that the $(n+1)$-special soundness extractor (see App. B) could extract a secret key V, and since the commitment scheme is perfect hiding, with probability $1/q_v$, V is the secret key corresponding to $Q_t = T_2$. In this case, we have

$$\begin{gathered}\log_{Q_t} V = \log_G P \\ \Downarrow \\ \log_{bG} V = \log_G aG \\ \Downarrow \\ V = abG\end{gathered}$$

Hence, V is a correct answer for the instance of the CDHP, and the proof is a PPT algorithm to find it with non-negligible probability. Consequently, under the CDHP assumption, our ID-based linkable ring signature scheme is unforgeable on adaptively chosen message and ID attacks. □

Theorem 4. *The scheme is of linkability in the random oracle model if the CDHP is intractable to solve. More specifically, if a PPT adversary grasps only one key pair (Q_t, V_t), then with negligible probability it can generate an accepting signature $\sigma = (cmt, x, rsp, I)$ on the event description event, such that $I \neq e(V, \mathcal{H}_2(event))$.*

Proof. On receiving an instance of CDHP $T = (G, T_1, T_2) = (G, aG, bG)$, the challenger $\mathcal{C}$ works as follows to simulate an unforgeability game for the PPT adversary $\mathcal{A}$.

The challenger $\mathcal{C}$ first provides the public system parameter to $\mathcal{A}$ which is supposed to forge an accepting signature with non-negligible probability ϵ such that $I \neq e(V, \mathcal{H}_2(event))$. To this end, $\mathcal{C}$ directly uses the group description $(\mathbb{G}, G, p, q)$ of the CDHP. Then it selects $H \leftarrow \mathbb{G}$, and set the master public key $P = T_1$. Fi-

nally, $pp = (\mathbb{G}, G, P, p, q, \mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, e)$ will be published, where the hash functions are modeled as random oracles.

Random oracle $\mathcal{H}(s)$: the random oracle is simulated the same as in the proof of Theorem 2.

Random oracle $\mathcal{H}_1(\mathrm{ID})$: the random oracle is simulated the same as in the proof of Theorem 2.

Random oracle $\mathcal{H}_2(event)$:the random oracle is simulated the same as in the proof of Theorem 3.

Extracting oracle $\mathcal{EO}(\mathrm{ID}, \overline{Q})$: This oracle can only be queried by $\mathcal{A}$ once. If $\overline{Q} = Q_t$, abort. If $\mathcal{H}_1(\mathrm{ID}) = \overline{Q}$, the challenger returns $\overline{V} = \overline{\alpha}P$, where $\alpha \leftarrow \mathbb{Z}_p$.

Signing oracle $\mathcal{SO}(L, Q, \mu, event)$: if there is a public key in L obtained not from querying $\mathcal{H}_1$ or $Q \notin L$, the challenger refuses to answer. Else if $Q = Q_t$, the challenger $\mathcal{C}$ sets the linking tag to be $I = e(Q, \beta P)$ and uses the SHVZK simulator to generate an accepting signature. Else if $Q \neq Q_t$, the challenger runs $\mathbf{Sign}(L, V = \alpha P, \mu, event)$ to generate an accepting signature. Otherwise, $\mathcal{C}$ refuses to answer.

Finally, $\mathcal{A}$ will return an accepting signature $\sigma^* = (\ldots, I)$ on L^*, μ^*, $event^*$ with non-negligible probability ϵ, such that σ^* was not generated by $\mathcal{SO}$ and $I \neq e(\overline{V}, \mathcal{H}_2(event^*))$.

Similar to the introduction in Theorem 3, C is able to extract an index t' and an element V^* such that $\log_{Q_{t'}} V^* = \log_G P = \log_{e(Q_{t'}, H_2(event^*))} I$. Similarly, with probability at least $1/q_v$, we have $t = t'$, so that

$$\log_{Q_t} V^* = \log_G P = a = \log_{e(Q_t, H_2(event^*))} I \ .$$

Thus, $V^* = aQ_t = abG$. Additionally, since $I \neq e(\overline{V}, \mathcal{H}_2(event^*))$, we have

$$\begin{aligned} \log_{Q_t} \overline{V} &= \log_{e(Q_t, \mathcal{H}_2(event^*))} e(\overline{V}, \mathcal{H}_2(event^*)) \\ &\neq \log_{e(Q_t, H_2(event^*))} I = \log_{Q_t} V^* \ . \end{aligned}$$

Hence, $\overline{V} \neq V^*$, which means V^* is a valid solution for the instance of the CDHP and $\mathcal{A}$ did not hold it in advance. With the CDHP assumption, $\mathcal{A}$ does not exist, so that the scheme is of linkability. □

Theorem 5. *The ID-based linkable ring signature scheme is nonslanderable in the random oracle model if it is unforgeable on adaptively chosen message and ID attacks and is of linkability.*

Proof. Theorem 3 showed that if an PPT adversary $\mathcal{A}$ does not hold one of secret key of the corresponding ring, it barely can generate an accepting signature. Thus, conditioned on $\mathcal{A}$ outputs an accepting signature $\sigma = (cmt, x, rsp, I)$ on behalf of L and event description $event$, it is with overwhelming probability that $\mathcal{A}$ made use the knowledge of its key pair (V, Q), such that $V \in L$. Then, by the proof of Theorem 4, the linking tag $I = e(V, \mathcal{H}_2(event))$ with overwhelming probability. To summarize, an PPT adversary $\mathcal{A}$ has negligible probability to output an accepting signature such that the linking tag is equivalent to the one belongs to another signer. □

4 Conclusions and Future Works

In this paper, we proposed an ID-based linkable ring signature with logarithmic size and gave a complete security proof to it. Without public key infrastructure, e-commerce parties are more flexible to deploy our signature in there system, and due to the logarithmic size, anonymity problems could be handled at the relatively low cost. In the future works, we are going to widely utilize the advantages of the current signature scheme. Several novel and practical applications are on route.

Acknowledgements

This work is supported by the National Key R&D Program of China (No. 2017YFB0802500) and the National Natural Science Foundation of China (No. 61672550, No. 61972429) and Guangdong Major Project of Basic and Applied Basic Research (No. 2019B030302008).

References

1. Au, M.H., Liu, J.K., Susilo, W., Yuen, T.H.: Constant-size ID-based linkable and revocable-iff-linked ring signature. In: Progress in Cryptology—INDOCRYPT 2006. pp. 364–378. Springer Berlin Heidelberg (2006)
2. Au, M.H., Liu, J.K., Susilo, W., Yuen, T.H.: Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theoretical Computer Science 469, 1 – 14 (2013)

3. Au, M.H., Liu, J.K., Yuen, T.H., Wong, D.S.: Id-based ring signature scheme secure in the standard model. In: Advances in Information and Computer Security. pp. 1–16. Springer Berlin Heidelberg (2006)
4. Awasthi, A.K., Lal, S.: ID-based ring signature and proxy ring signature schemes from bilinear pairings. International Journal of Network Security 4(2), 187–192 (2007)
5. Backes, M., Döttling, N., Hanzlik, L., Kluczniak, K., Schneider, J.: Ring signatures: Logarithmic-size, no setup—from standard assumptions. In: Advances in Cryptology—EUROCRYPT 2019. pp. 281–311. Springer International Publishing (2019)
6. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Theory of Cryptography—TCC 2006. pp. 60–79. Springer Berlin Heidelberg (2006)
7. Beullens, W., Katsumata, S., Pintore, F.: Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In: Advances in Cryptology – ASIACRYPT 2020. pp. 464–492. Springer International Publishing (2020)
8. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Advances in Cryptology—CRYPTO 2001. pp. 213–229. Springer Berlin Heidelberg (2001)
9. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J., Petit, C.: Short accountable ring signatures based on DDH. In: Computer Security—ESORICS 2015. pp. 243–265. Springer International Publishing (2015)
10. Chatterjee, R., Garg, S., Hajiabadi, M., Khurana, D., Liang, X., Malavolta, G., Pandey, O., Shiehian, S.: Compact ring signatures from learning with errors. Cryptology ePrint Archive, Report 2021/942 (2021), https://ia.cr/2021/942
11. Chengyu Hu, Pengtao Liu: An enhanced constant-size identity-based ring signature scheme. In: 2nd IEEE International Conference on Computer Science and Information Technology. pp. 587–590. IEEE (2009)
12. Chow, S.S.M., Wei, V.K., Liu, J.K., Yuen, T.H.: Ring signatures without random oracles. In: Symposium on Information, Computer and Communications Security. pp. 297–302. ASIACCS '06, ACM, New York, NY, USA (2006)
13. Chow, S.S.M., Yiu, S.M., Hui, L.C.K.: Efficient identity based ring signature. In: Applied Cryptography and Network Security—ACNS 2005. pp. 499–512. Springer Berlin Heidelberg (2005)
14. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in Ad Hoc groups. In: Advances in Cryptology—EUROCRYPT 2004. pp. 609–626. Springer Berlin Heidelberg (2004)

15. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology—CRYPTO 1986. pp. 186–194. Springer Berlin Heidelberg (1987)
16. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: Symposium on Theory of Computing—STOC 1985. pp. 291–304. ACM (1985)
17. Groth, J., Kohlweiss, M.: One-out-of-many proofs: Or how to leak a secret and spend a coin. In: Advances in Cryptology—EUROCRYPT 2015. pp. 253–280. Springer Berlin Heidelberg (2015)
18. Haque, A., Krenn, S., Slamanig, D., Striecks, C.: Logarithmic-size (linkable) threshold ring signatures in the plain model. Cryptology ePrint Archive, Report 2020/683 (2020), https://ia.cr/2020/683
19. Libert, B., Peters, T., Qian, C.: Logarithmic-size ring signatures with tight security from the DDH assumption. In: Computer Security—USORICS 2018. pp. 288–308. Springer International Publishing (2018)
20. Libert, B., Nguyen, K., Peters, T., Yung, M.: One-shot fiat-shamir-based nizk arguments of composite residuosity in the standard model. Cryptology ePrint Archive, Report 2020/1334 (2020), https://ia.cr/2020/1334
21. Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Linkable ring signature with unconditional anonymity. IEEE Transactions on Knowledge and Data Engineering 26(1), 157–165 (Jan 2014)
22. Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: Computational Science and Its Applications—ICCSA 2005. pp. 614–623. Springer Berlin Heidelberg (2005)
23. Lyubashevsky, V., Nguyen, N.K., Seiler, G.: Smile: Set membership from ideal lattices with applications to ring signatures and confidential transactions. Cryptology ePrint Archive, Report 2021/564 (2021), https://ia.cr/2021/564
24. Nguyen, L.: Accumulators from bilinear pairings and applications. In: Topics in Cryptology—CT-RSA 2005. pp. 275–292. Springer Berlin Heidelberg (2005)
25. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology—CRYPTO 1991. pp. 129–140. Springer Berlin Heidelberg (1992)
26. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Advances in Cryptology—ASIACRYPT 2001. pp. 552–565. Springer Berlin Heidelberg (2001)
27. Saberhagen, N.v.: CryptoNote v2.0 (2013), https://cryptonote.org/whitepaper.pdf
28. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from Bitcoin. In: Symposium on Security and Privacy—SP 2014. pp. 459–474. IEEE (May 2014)

29. Zhang, F., Chen, X.: Cryptanalysis and improvement of an ID-based ad-hoc anonymous identification scheme at CT-RSA 05. Information Processing Letters 109(15), 846 – 849 (2009)

30. Zhang, F., Kim, K.: Id-based blind signature and ring signature from pairings. In: Advances in Cryptology—ASIACRYPT 2002. pp. 533–547. Springer Berlin Heidelberg (2002)

31. Zhang, H., Zhang, F., Tian, H., Au, M.H.: Anonymous post-quantum cryptocash. In: Financial Cryptography and Data Security—FC 2018. pp. 461–479. Springer Berlin Heidelberg (2018), full version at https://eprint.iacr.org/2017/716

Appendix

A Proof of Theorem 1

Proof. It is easy to see that a signature which is honestly generated by a valid signatory can always pass the verification procedure **Vfy**. We only explicitly deduce the two equations whose correctness are not shown directly. The first equation is responsible for checking that the linking tag is generated honestly.

$$\begin{aligned} x^m I - \sum_{k=0}^{m-1} x^k E_k &= x^n \cdot e(V_\ell, K) - e(P, \sum_{k=0}^{n-1} x^k \rho_k K) \\ &= e(x^n V_\ell, K) - e(\sum_{k=0}^{n-1} x^k \rho_k P, K) \\ &= e(x^n V_\ell - \sum_{k=0}^{n-1} x^k \rho_k P, K) \\ &= e(Z, K) \ . \end{aligned}$$

The second equation is to show that the signer hold the corresponding signing key.

$$
\begin{aligned}
& e\left(\sum_{i=0}^{n-1}(\prod_{j=1}^{m} w_{j,i_j})Q_i + \sum_{k=0}^{m-1}(-x^k)D_k, P\right) \\
&= e\left(\sum_{i=0}^{n-1}(\delta_{i\ell}x^m + \sum_{k=1}^{m-1} p_{i,k}x^k)Q_i - \sum_{k=0}^{m-1}((\sum_{i=0}^{n-1} p_{i,k}Q_i) + \rho_k G)x^k, P\right) \\
&= e\left(\sum_{i=0}^{n-1}\delta_{i\ell}x^m Q_i - \sum_{k=0}^{m-1}\rho_k x^k G, P\right) \\
&= e\left(x^m Q_\ell - \sum_{k=0}^{m-1}\rho_k x^k G, vG\right) \\
&= e\left(x^m V_\ell - \sum_{k=0}^{m-1}\rho_k x^k P, G\right) \\
&= e\,(Z, G)
\end{aligned}
$$

The correctness of the other equations could be verified easily. □

B The Underlying Sigma-Protocol

We have noticed before that the current ID-based linkable ring signature scheme is the non-interactive version of a one-out-of many Sigma-protocol which we call it Σ_2. The only difference between them is that in the Sigma-protocol, the hash digest $x \in \mathbb{Z}_p$ is chosen uniformly at random by the verifier rather than computed from some predetermined values. Such a framework is inspired by [17], and actually, to build the aforementioned one-out-of-many Sigma-Protocol, another Sigma-Protocol (which we call it Σ_1 for short) for proving that a commitment is opened to 1 or 0 is needed. As Σ_1 is the same to the one in Sect. 2.3 in [17], we omit its description here. The only thing we need to know is that σ_1 is perfect 2-special sound and perfect special honest verifier zero-knowledge.

Given the public parameters pp, public keys $Q_0, \ldots, Q_{n-1}$, linking tag $I = e(V_\ell, K)$, and the event description $event$ which fixes $K = \mathcal{H}_2(event)$, the NP relation to be proved by the prover (signer) who hold $V_\ell = vQ_\ell$ is

$$
\mathcal{R} = \left\{ (pp, (Q_0, \ldots, Q_{n-1}, K, I), (\ell, V_\ell)) : \begin{array}{r} Q_1, \ldots, Q_n, \in \mathbb{G} \wedge \ell \in [0, n) \wedge \\ I \in \mathbb{G}_T \wedge \log_{Q_\ell} V_\ell = \log_G P \wedge \\ \log_{e(Q_\ell, K)} I = \log_G P \end{array} \right\} .
$$

In simple terms, the prover should convince the verifier that 1) his/her knowledge to the NP witness involves an integer $\ell \in [0, n)$ and a group element $V_\ell \in \mathbb{G}$; 2) the discrete logarithm between V_ℓ and the ℓth public key Q_ℓ is equal to that between the master public key P and the group generator G; 3) The linking tag is uniquely determined by V_ℓ under the same *pp* and *event*.

Theorem 6. *Σ_2 is of $(m+1)$-special soundness.*

Proof. Suppose the adversary creates $m+1$ accepting responses

$$\{w_1^{(\alpha)}, \ldots, w_m^{(\alpha)}, y_1^{(\alpha)}, \ldots, y_m^{(\alpha)}, z_1^{(\alpha)}, \ldots, , z_m^{(\alpha)}, Z^{(\alpha)}\}_{\alpha \in [0,m]}$$

to $m+1$ distinct challenges $x^{(0)}, \ldots, x^{(m)}$. Using any two of the challenge-response pairs, the 2-special soundness of Σ_1 ensures that we are able to extract an opening $(\ell_j, r_j) \in \{0,1\} \times \mathbb{Z}_p$ to A_j such that for $j \in [1, m]$, $A_j = \ell_j H + r_j G$. Additionally, from the first equation in the verification, we have

$$\begin{aligned}
x^{(\alpha)} A_j + B_j &= w_j^{(\alpha)} H + y_j^{(\alpha)} G \\
&\Downarrow \\
B_j &= w_j^{(\alpha)} H + y_j^{(\alpha)} G - x^{(\alpha)} A_j \\
&\Downarrow \\
B_j &= w_j^{(\alpha)} H + y_j^{(\alpha)} G - x^{(\alpha)} (\ell_j H + r_j G) \\
&\Downarrow \\
B_j &= (w_j^{(\alpha)} - x^{(\alpha)} \ell_j) H + (y_j^{(\alpha)} - x^{(\alpha)} r_j) G.
\end{aligned}$$

Define $a_j^{(\alpha)} = w_j^{(\alpha)} - x^{(\alpha)} \ell_j$, and it is with overwhelming probability that $a_j^{(\alpha)} = a_j^{(\alpha')} \stackrel{\text{def}}{=} a_j$ for all $\alpha, \alpha' \in [0, m]$ (otherwise, we obtain at least one pair of distinct openings to B_j). Consequently, we have that $w_j^{(\alpha)} = \ell_j x^{(\alpha)} + a_j$ for all $\alpha \in [0, m]$ and $j \in [1, m]$. For $i \neq \ell$, we can see that $\prod_{j=1}^m w_{j,i_j}^{(\alpha)}$ is a degree $m-1$ polynomial in determinate x and for $i = \ell$, it is a polynomial of degree m. So, from the last equation in the verification procedure, we have

$$\begin{aligned}
& e\left(\sum_{i=0}^{n-1} (\prod_{j=1}^{m} w_{j,i_j}^{(\alpha)}) Q_i + \sum_{k=0}^{m-1} (-(x^{(\alpha)})^k) D_k, P \right) \\
&= e\left((x^{(\alpha)})^m Q_\ell + \sum_{i=0}^{n-1} \sum_{k=0}^{m-1} p_{i,k} (x^{(\alpha)})^k Q_i - \sum_{k=0}^{m-1} (x^{(\alpha)})^k D_k, P \right) \\
&= e\left((x^{(\alpha)})^m Q_\ell + \sum_{k=0}^{m-1} (x^{(\alpha)})^k D'_k, P \right) \\
&= e\left(Z^{(\alpha)}, G \right) \quad ,
\end{aligned}$$

where the third line of the above equation could be viewed as a polynomial of degree m with indeterminate $x^{(\alpha)}$, and D'_k is the coefficient of the k-th degree term. Since $x^{(0)}, \ldots, x^{(m)}$ are all different, we can find $\beta_0, \beta_1, \ldots, \beta_m$ so that the following equation holds.

$$\begin{pmatrix} (x^{(0)})^0 & (x^{(1)})^0 & \ldots & (x^{(m)})^0 \\ (x^{(0)})^1 & (x^{(1)})^1 & \ldots & (x^{(m)})^1 \\ \vdots & \vdots & \ddots & \vdots \\ (x^{(0)})^m & (x^{(1)})^m & \ldots & (x^{(m)})^m \end{pmatrix} \cdot \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} .$$

Define $V'_\ell = \sum_{\alpha=0}^{m} \beta_\alpha Z^{(\alpha)}$. Notice that

$$\begin{aligned} e(V'_\ell, G) &= e\left(\sum_{\alpha=0}^{m} \beta_\alpha \cdot Z^{(\alpha)}, G\right) \\ &= e\left(\sum_{\alpha=0}^{m} \beta_\alpha \left((x^{(\alpha)})^m Q_\ell + \sum_{k=0}^{m-1} (x^{(\alpha)})^k D'_k\right), P\right) \\ &= e\left(\sum_{\alpha=0}^{m} \left(\beta_\alpha (x^{(\alpha)})^m\right) Q_\ell + \sum_{k=0}^{m-1} \left(\sum_{\alpha=0}^{m} \beta_\alpha (x^{(\alpha)})^k\right) D'_k, P\right) \\ &= e\left(Q_\ell, P\right) \\ &= e\left(vQ_\ell, G\right). \end{aligned}$$

So we conclude that $V'_\ell = vQ_\ell$. On the other side, from the equation which is responsible for checking the validity of linking tag, we have

$$\left(x^{(\alpha)}\right)^n I - e\left(P, \sum_{k=0}^{n-1} \left(x^{(\alpha)}\right)^k E_k\right) = e(Z^{(\alpha)}, K) \ ,$$

so that with the $m+1$ accepting transcripts, we obtain

$$\begin{pmatrix} 1 & (x^{(0)})^1 & \cdots & (x^{(0)})^m \\ 1 & (x^{(1)})^1 & \cdots & (x^{(1)})^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x^{(m)})^1 & \cdots & (x^{(m)})^m \end{pmatrix} \begin{pmatrix} E_0 \\ E_1 \\ \vdots \\ I \end{pmatrix} = \begin{pmatrix} e(Z^{(0)}, K) \\ e(Z^{(1)}, K) \\ \vdots \\ e(Z^{(m)}, K) \end{pmatrix} . \tag{1}$$

By left multiplying (1) with $(\beta_0, \beta_1, \ldots, \beta_m)$, we observe that

$$I = \sum_{\alpha=0}^{m} \beta_\alpha \cdot e\left(Z^{(\alpha)}, K\right) = e\left(\sum_{\alpha=0}^{m} \beta_\alpha \cdot Z^{(\alpha)}, K\right) = e(V'_\ell, K) = v \cdot e(Q_\ell, K) \ .$$

The above facts show that (ℓ, V'_ℓ) is a valid witness for the statement in $\mathcal{R}$. $\square$

Theorem 7. *Σ_2 is of special honest verifier zero-knowledge (SHVZK) if the commitment scheme is perfect hiding.*

Proof. On input a challenge $x \in \mathbb{Z}_p$, the simulator first chooses $w_j, y_j, z_j \leftarrow \mathbb{Z}_p$, for $j \in [1, m]$, and $s \leftarrow \mathbb{Z}_p$. The simulator computes $Z = sP$. It is obvious that the distributions of these simulated responses are statistically close to that in a real proof. The simulator then picks $\ell \leftarrow [0, n)$, $r_j \leftarrow \mathbb{Z}_p$ and computes $A_j = \ell_j H + r_j G$. Due to the properties of the commitment scheme, $(r_j)_{j=1}^{\tau}$ are statistically indistinguishable from that of a real proof.

Subsequently, for $j \in [1, \tau]$, let $a_j = f_j - \ell_j x$, and compute $(p_{i,j})_{i \in [0,n), k \in [1,m)}$. For $k \in [1, \tau)$, it picks $\rho_k \leftarrow \mathbb{Z}_p$ and computes $D_k = \sum_{i=0}^{n-1} p_{i,k} Q_i + \rho_k G$, $E_k = e(P, \rho_k K)$. The distributions of D_k and E_k are statistically close to uniform distribution in G and they are pairwise dependent since they use the same randomness as in a real proof.

Since $(B_j)_{j=1}^m$, $(C_j)_{j=1}^m$, D_0, E_0 are uniquely determined by the corresponding verification equations and the above generated parameters, the simulator computes

$$
\begin{aligned}
B_j &= w_j H + y_j G - x A_j \ \ , \text{ for } j \in [1, m] \\
C_j &= z_j G - (x - w_j) A_j \ \ , \text{ for } j \in [1, m] \\
D_0 &= \sum_{i=0}^{n-1} (\prod_{j=1}^{m} w_{j,i_j}) Q_i + \sum_{k=1}^{m-1} (-x^k) D_k - rG \\
E_0 &= x^m I - \sum_{k=1}^{m-1} x^k - e(Z, K) \ \ .
\end{aligned}
$$

By the foregoing discussion, the distribution of the outputting transcript

$$
\big((A_j, B_j, C_j), D_{j-1}, E_{j=1}^m, x, (w_j)_{j=1}^m, (y_j)_{j=1}^m, (z_j)_{j=1}^m, Z\big)
$$

is totally indistinguishable from that of a real proof. As a result, Σ_2 is SHVZK. $\square$