Identity-Based Revocable and Linkable Ring Signature

Muyuan Wang[1,2][0009−0005−1048−8067]

[1] Hubei University, Wuhan 430062, China
[2] Beijing Infosec Technologies Co. Ltd., Beijing 100096, China
mywang2026@126.com

Abstract. Revocable and linkable ring signatures (RLRS) provide a practical mechanism for controllable anonymity, enabling a revocation authority (RA) to mandatorily revoke the anonymity of the real signer. However, existing constructions often rely on the assumption of a fully trusted RA, where the correctness of the revocation is not publicly verifiable rendering honest users vulnerable to undetected framing by a compromised RA. Furthermore, the concrete deployment of these schemes is hindered by the certificate management burden of PKI and computation or communication overheads that scale linearly with the ring size, limiting their real-world applicability.
In this paper, we formalize the notion of Identity-Based Revocable and Linkable Ring Signatures (IB-RLRS), inherently eliminating cumbersome PKI management. Our primary contribution is the enhancement of *revocability* alongside a newly adapted property termed *revocation soundness*, guaranteeing that the real signer's identity can always be extracted, and that a malicious RA cannot frame honest users who did not participate in the signature generation. We present an efficient instantiation of IB-RLRS scheme, and prove its security in the random oracle model. Specifically, a novel ring signature construction is proposed, which features a transparent setup and achieves a logarithmic signature size, demonstrating its feasibility for large-scale, privacy-preserving applications.

Keywords: Ring signature · Identity-based cryptography · Revocability · Logarithmic size

1 Introduction

Introduced by Rivest *et al.* [19], ring signatures extend the functionality of standard digital signatures by enabling signer anonymity. A user can spontaneously form a set of public keys and produce a signature, while the actual signer remains hidden within that set. Compared with group signatures [9], ring signatures do not require any group manager or setup phase, making them particularly suitable for ad-hoc and decentralized environments.

While widely deployed in privacy-preserving applications such as e-voting and confidential transactions, classical ring signatures provide unconditional anonymity, meaning that the real signer cannot be identified once the signature

is produced. This limitation can be exploited maliciously, motivating the study of enhanced variants with controllable anonymity [16, 11, 15, 4, 22, 17]. Recently, Zhang *et al.* [24] formalized the notion of RLRS. Their framework enables a RA to mandatorily revoke the anonymity of a signature in constant time. Simultaneously, it allows anyone to publicly link signatures produced by the same signer under the same event to prevent double spending. To demonstrate its practical applicability in privacy enhancing technologies, they further extended the RLRS scheme into a revocable ring confidential transaction protocol, facilitating the construction of blockchain systems that comply with regulatory requirements.

1.1 Related Work

The development of the RLRS framework builds upon a series of enhancements designed to achieve controllable anonymity. Initially, Liu et al. [16] proposed the linkable ring signature (LRS) to detect double spending. To provide further regulation, Fujisaki and Suzuki [11] introduced traceable ring signatures, which reveal the signer's identity only if they endorse different messages. As this conditional traceability falls short for on-demand revocation, Liu *et al.* [15] proposed revocable ring signatures, designating revokers to extract the signer's identity. Bootle *et al.* [4] later formalized accountable ring signatures to allow an independent opener to extract identities and provide correctness proofs, though their scheme inherently requires unlinkability. To mitigate centralized regulatory power, Zhaolu *et al.* [25] introduced controllable linkable ring signatures to separate privileges. These foundational works culminated in the RLRS framework, with recent optimizations like [14] further enhancing performance.

Limitations of Existing RLRS Schemes. Despite providing controllable anonymity, the real-world deployment of existing RLRS schemes remains constrained by restrictive security models and inherent certificate management overhead of PKI. On the one hand, standard revocability definitions limit the adversary's corruption capability, failing to capture real-world collusion attacks. Furthermore, these models implicitly assume a fully trusted RA, rendering the revocation process publicly unverifiable and leaving honest users vulnerable to undetected framing. On the other hand, most RLRS schemes are confined to the traditional PKI setting. The immense certificate management overhead makes them unsuitable for highly scalable and decentralized environments.

The Quest for Efficient Identity-Based RLRS. Identity-based cryptography [20] offers an alternative to eliminate the PKI burden. However, migrating ring signatures to the ID-based setting introduces an inherent trade-off between signature size and transparent setup. Early IBRS constructions (e.g., [23, 5]) feature concise setups but exhibit computational and communication overheads that scale linearly with the ring size. Accumulator-based schemes [18] successfully compress signatures to a constant size, but at the expense of introducing a trapdoor key escrow vulnerability. Recently, building on the techniques of [12], Nassurdine *et al.* [17] proposed a transparent ID-based linkable ring signature scheme with logarithmic size. Nevertheless, this approach relies on complex underlying zero-knowledge proofs, incurring heavy computational complexity. This

stands in contrast to the PKI setting, where numerous efficient logarithmic-size ring signature schemes have been proposed [22, 13, 3].

1.2 Our Contributions

The main contributions of this work are summa- rized as follows:

1. **Formalization of the IB-RLRS.** We formalize the notion of Identity-Based Revocable and Linkable Ring Signatures (IB-RLRS). We strengthen *revocability* to guarantee that the actual signer's identity can always be extracted by the RA, even under the full compromise of all ring keys. Furthermore, we introduce *revocation soundness*, a notion adapted from accountable ring signatures, to ensure that even a fully corrupted RA cannot frame an honest user who did not participate in the signature generation.
2. **Construction with Transparent Setup.** We present an efficient construction of the IB-RLRS, denoted BLMQ-RLRS, together with a formal security analysis in the random oracle model. Our construction integrates the BLMQ signature scheme [1], the set membership proof [22], and the Twisted ElGamal encryption [10]. Our novel construction achieves logarithmic signature size without requiring trusted setup in the ID-based setting.

2 Preliminaries

2.1 Notions

Let λ denote the security parameter, and probabilistic polynomial-time algorithms are abbreviated as PPT. Let $\{0,1\}^*$ denote the set of all finite binary strings, and $\mathsf{event} \in \{0,1\}^*$ be the event description that specifies the context of the signature. We write $s \leftarrow\!\$\ \mathbb{S}$ to denote that s is sampled uniformly at random from $\mathbb{S}$. A function $\mathsf{negl}(\lambda)$ is *negligible* in λ if for every polynomial $p(\cdot)$, there exists N such that for all $\lambda > N$, $\mathsf{negl}(\lambda) \leq 1/p(\lambda)$.

For $n \in \mathbb{N}$, let $[n] = \{1, 2, \ldots, n\}$. Let $\mathbb{F}$ be a finite field, and $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}^n$ denote an n-dimensional vector over $\mathbb{F}$, where $a_i \in \mathbb{F}$. For $y \in \mathbb{F}$ and $n \in \mathbb{N}$, let $\boldsymbol{y}^n = (1, y, y^2, \ldots, y^{n-1})$. A binary vector is called one-hot if it contains exactly one entry equal to 1 and all others equal to 0.

2.2 Bilinear Pairing

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be cyclic groups of prime order q, with generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$. A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is called a bilinear pairing if it satisfies the following properties:

1. Bilinear: For all $a, b \in \mathbb{Z}_q$ we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
2. Non-degenerate: $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$.
3. Efficiently computable: For any $h_1 \in \mathbb{G}_1$ and $h_2 \in \mathbb{G}_2$, there exists an efficient algorithm to compute $e(h_1, h_2)$.

Furthermore, the bilinear pairing e is said to be of Type II if $\mathbb{G}_1 \neq \mathbb{G}_2$ and there exists an efficiently computable isomorphism $\phi : \mathbb{G}_2 \to \mathbb{G}_1$. We denote the Type II bilinear group as $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e, \phi)$.

q-Strong Diffie-Hellman (q-SDH) Assumption: For an unknown $s \in \mathbb{Z}_q$ and a tuple $(g_1, g_2, g_2^s, \ldots, g_2^{s^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^q$, it is hard to compute a pair $(g_1^{\frac{1}{s+x}}, x)$ for some $x \in \mathbb{Z}_q$.

q-Decisional Bilinear Diffie-Hellman Inversion (q-DBDHI) Assumption: For an unknown $s \in \mathbb{Z}_q$ and a tuple $(g_1, g_2, g_2^s, \ldots, g_2^{s^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^q$, it is hard to distinguish $e(g_1, g_2)^{\frac{1}{s}}$ from a random element in $\mathbb{G}_T$.

Background on IEEE P1363 signature scheme [1], Twisted ElGamal encryption [10], and Signatures of Knowledge is provided in Appendix A.

3 Identity-Based Revocable and Linkable Ring Signature

In this section we formalize the syntax of identity-based revocable and linkable ring signature(IB-RLRS), and define its security model.

3.1 Syntax

An IB-RLRS scheme involves four entities: the KGC, the RA, the signer and the verifier, and it consists of eight algorithms (Setup, RevokeKeyGen, KeyExt, Sign, Verify, Link, Revoke, Judge).

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$: On input a security parameter λ, the KGC generates and publishes the public parameters pp, while secretly retaining the master secret key msk. Assume pp is implicitly provided to all subsequent algorithms.
- $(\mathsf{pk}_R, \mathsf{sk}_R) \leftarrow \mathsf{RevokeKeyGen}(\mathsf{pp})$: The RA generates the keypair $(\mathsf{pk}_R, \mathsf{sk}_R)$, used to trace the actual signer during disputes.
- $d_{\mathsf{ID}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \mathsf{ID})$: The KGC takes as input the msk and an identity $\mathsf{ID} \in \{0,1\}^*$, outputs the private key d_{ID} associated with the identity ID.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{event}, \mathsf{pk}_R, d_{\mathsf{ID}}, L, m)$: The signer takes as input the event, the RA's public key pk_R, its private key d_{ID}, a ring L of identities with $\mathsf{ID} \in L$, and a message m, outputs a signature σ.
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma)$: The verifier takes as input the event, the RA's public key pk_R, the ring L, the message m and the signature σ. It outputs 1 if σ is valid, and 0 otherwise.
- $\{0,1\}/\perp \leftarrow \mathsf{Link}(\mathsf{event}, \mathsf{pk}_{R1}, \mathsf{pk}_{R2}, L_1, L_2, m_1, m_2, \sigma_1, \sigma_2)$: On input two tuples $(L_i, m_i, \sigma_i, \mathsf{pk}_{Ri}), i \in \{0,1\}$ and the event, outputs $\perp$ if either signature is invalid. Otherwise, outputs 1 if the signatures are linked, and 0 otherwise.
- $(\mathsf{ID}, \pi)\ /\ \perp \leftarrow \mathsf{Revoke}(\mathsf{event}, \mathsf{sk}_R, L, m, \sigma)$: The RA takes as input a tuple (L, m, σ) under the event, and its private key sk_R, outputs $\perp$ if the signature is invalid. Otherwise, outputs the real identity $\mathsf{ID} \in L$ of the signer together with a zero-knowledge proof π.

– $\{0,1\}/\perp \leftarrow \mathsf{Judge}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma, \mathsf{ID}, \pi)$: On input a tuple (L, m, σ) under the event, and a claimed identity ID with proof π, this algorithm outputs $\perp$ if the signature is invalid. Otherwise, outputs 1 if π is a valid proof that $\mathsf{ID} \in L$ is the signer of σ, and 0 otherwise.

Correctness: An IB-RLRS scheme should satisfy the following requirements:

– Verification Correctness: For any $\mathsf{event}, m, \mathsf{pk}_R$, and L such that $\mathsf{ID} \in L$, letting $\sigma \leftarrow \mathsf{Sign}(\mathsf{event}, \mathsf{pk}_R, d_{\mathsf{ID}}, L, m)$, we have:

$$\Pr\left[\mathsf{Verify}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma) = 1\right] = 1.$$

– Link Correctness: For any $\mathsf{event}, \mathsf{pk}_{R1}, \mathsf{pk}_{R2}, m_1, m_2$, and L_1, L_2 such that $\mathsf{ID} \in L_1 \cap L_2$, letting $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{event}, \mathsf{pk}_{Ri}, d_{\mathsf{ID}}, L_i, m_i)$, $i \in \{1,2\}$, we have:

$$\Pr\left[\mathsf{Link}(\mathsf{event}, \mathsf{pk}_{R1}, \mathsf{pk}_{R2}, L_1, L_2, m_1, m_2, \sigma_1, \sigma_2) = 1\right] = 1.$$

– Revocation Correctness: For any event, m, and L such that $\mathsf{ID} \in L$, letting $\sigma \leftarrow \mathsf{Sign}(\mathsf{event}, \mathsf{pk}_R, d_{\mathsf{ID}}, L, m)$, $(\mathsf{ID}', \pi) \leftarrow \mathsf{Revoke}(\mathsf{event}, \mathsf{sk}_R, L, m, \sigma)$, we have:

$$\Pr\left[\mathsf{ID}' = \mathsf{ID} \wedge \mathsf{Judge}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma, \mathsf{ID}', \pi) = 1\right] = 1.$$

3.2 Security Requirements

Analogous to conventional RLRS and ARS constructions, an IB-RLRS scheme is required to satisfy unforgeability, anonymity, linkability, non-frameability, revocability, and revoking soundness. We formalize these notions by extending the standard security models from [2, 4, 24] to the identity-based setting.

In the security models, we assume the adversary $\mathcal{A}$ can adaptively interact with the challenger $\mathcal{C}$. To formally define the non-triviality of the attacks, the challenger initializes empty lists $\mathcal{Q}_{\mathsf{H}}$, $\mathcal{Q}_{\mathsf{KeyExt}}$, $\mathcal{Q}_{\mathsf{Sign}}$, and $\mathcal{Q}_{\mathsf{Revoke}}$ to track the interactions with the oracles, defined as follows:

– $\mathcal{O}_{\mathsf{H}}(x)$: On input a string x, if $(x, h) \in \mathcal{Q}_{\mathsf{H}}$, $\mathcal{C}$ returns h. Otherwise, it samples a random h from the target space, records (x, h) in $\mathcal{Q}_{\mathsf{H}}$, and returns h to $\mathcal{A}$.
– $\mathcal{O}_{\mathsf{KeyExt}}(\mathsf{ID})$: On input an identity ID, $\mathcal{C}$ computes $d_{\mathsf{ID}} \leftarrow \mathsf{KeyExt}(\mathsf{msk}, \mathsf{ID})$. It then adds ID to the corrupted list $\mathcal{Q}_{\mathsf{KeyExt}}$ and returns d_{ID} to $\mathcal{A}$.
– $\mathcal{O}_{\mathsf{Sign}}(\mathsf{event}, L, \mathsf{ID}, m)$: $\mathcal{C}$ computes a valid signature σ on (m, event) under $\mathsf{ID} \in L$, records $(\mathsf{event}, L, \mathsf{ID}, m, \sigma)$ in $\mathcal{Q}_{\mathsf{sign}}$, and returns σ.
– $\mathcal{O}_{\mathsf{Revoke}}(\mathsf{event}, L, m, \sigma)$: On input a tuple $(\mathsf{event}, L, m, \sigma)$, $\mathcal{C}$ computes and returns the revocation outcome $(\mathsf{ID}, \pi_{dec})/\perp \leftarrow \mathsf{Revoke}(\mathsf{sk}_R, L, m, \sigma)$.

Unforgeability. No PPT adversary can successfully forge a valid signature on behalf of an uncorrupted user. In the game $\mathsf{SigForge}$, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows:

– **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and sends pp to $\mathcal{A}$. $\mathcal{A}$ computes the revoke keypair $(\mathsf{pk}_R, \mathsf{sk}_R)$ and sends pk_R to $\mathcal{C}$.

- **Query.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$.
- **Forge.** $\mathcal{A}$ outputs the tuple $(\mathsf{event}^*, L^*, M^*, \sigma^*)$. The game outputs 1 if:
  1. $\mathsf{Verify}(\mathsf{event}^*, \mathsf{pk}_R, L^*, M^*, \sigma^*) = 1$;
  2. All identities in L^* has not been queried to $\mathcal{O}_{\mathsf{KeyExt}}$;
  3. $\forall \mathsf{ID} \in L^*, (\mathsf{event}^*, L^*, \mathsf{ID}, M^*, \sigma) \notin \mathcal{Q}_{\mathsf{sign}}$.

The advantage of $\mathcal{A}$ in winning the game $\mathsf{SigForge}$ is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sigforge}}(\lambda) = \Pr\left[\mathsf{SigForge}_{\mathcal{A}}^{\mathsf{IB\text{-}RLRS}}(\lambda) = 1\right].$$

Definition 1 (Unforgeability). *An* IB-RLRS *scheme satisfies Existential Unforgeability against Adaptive Chosen Message and Identity Attacks(EUF-CMIA) if for any* PPT *adversary* $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sigforge}}(\lambda)$ *is negligible.*

Anonymity: No PPT adversary (other than the KGC and RA) can distinguish the actual signer. In the game $\mathsf{SigAnon}$, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows:

- **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and runs $\mathsf{RevokeKeyGen}(\mathsf{pp})$ to generate the revoke key pair $(\mathsf{pk}_R, \mathsf{sk}_R)$. Then, $\mathcal{C}$ sends pp and pk_R to $\mathcal{A}$.
- **Phase 1.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$, and $\mathcal{Q}_{\mathsf{Revoke}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$, and $\mathcal{O}_{\mathsf{Revoke}}$.
- **Challenge.** $\mathcal{A}$ outputs the challenge tuple $(M^*, \mathsf{event}^*, L^*)$ and two distinct indices $i_0, i_1 \in [1, n]$. For any $\mathsf{ID} \in \{\mathsf{ID}_{i_0}, \mathsf{ID}_{i_1}\}$, $\mathcal{A}$ must not have queried $\mathcal{O}_{\mathsf{KeyExt}}$ on ID nor $\mathcal{O}_{\mathsf{Sign}}$ on $(\cdot, \mathsf{event}^*, \cdot, \mathsf{ID})$. $\mathcal{C}$ samples $b \leftarrow\!\!\$\ \{0, 1\}$, generates a challenge signature σ^* on $(M^*, \mathsf{event}^*, L^*)$ under ID_{i_b}, and returns it to $\mathcal{A}$.
- **Phase 2.** $\mathcal{A}$ continues querying the oracles as in Phase 1, subject to the restrictions on $\mathsf{ID}_{i_0}, \mathsf{ID}_{i_1}$, and cannot query $\mathcal{O}_{\mathsf{Revoke}}$ on $(M^*, \mathsf{event}^*, L^*, \sigma^*)$.
- **Guess.** $\mathcal{A}$ outputs its guess b'. $\mathcal{A}$ wins the game if $b' = b$.

The advantage of the adversary in winning the game $\mathsf{SigAnon}$ is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{siganon}}(\lambda) = 2\left|\Pr[b' = b] - \frac{1}{2}\right|.$$

Definition 2 (Anonymity). *An* IB-RLRS *scheme satisfies anonymity if for any adversary* $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{siganon}}(\lambda)$ *is negligible.*

Linkability: No adversary can generate unlinkable ring signatures on behalf of the same user under the same event. In the linkability game $\mathsf{SigLink}$, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows:

- **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and sends pp to $\mathcal{A}$. $\mathcal{A}$ computes the revoke keypair $(\mathsf{pk}_R, \mathsf{sk}_R)$ and sends pk_R to $\mathcal{C}$.
- **Query.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$.
- **Forgery.** $\mathcal{A}$ outputs a tuple $(L_1, M_1, \sigma_1, L_2, M_2, \sigma_2, \mathsf{event}^*)$. Let $S_{corr} \subseteq L_1 \cup L_2$ be the set of identities queried to $\mathcal{O}_{\mathsf{KeyExt}}$. The game outputs 1 if:

1. $\mathsf{Verify}(\mathsf{event}^*, \mathsf{pk}_R, L_i, M_i, \sigma_i) = 1$ for $i \in \{1, 2\}$;
2. $\mathsf{Link}(\mathsf{event}^*, \mathsf{pk}_R, \mathsf{pk}_R, L_1, L_2, M_1, M_2, \sigma_1, \sigma_2) = 0$;
3. $|S_{corr}| \leq 1$;
4. $\mathcal{A}$ made no $\mathcal{O}_{\mathsf{Sign}}$ queries involving event^*.

The advantage of the adversary in winning the game SigLink is defined as

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{siglink}}(\lambda) = \Pr\left[\mathsf{SigLink}_{\mathcal{A}}^{\mathsf{IB\text{-}RLRS}}(\lambda) = 1\right]$$

Definition 3 (Linkability). *An* IB-RLRS *scheme satisfies linkability if for any adversary* $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{siglink}}(\lambda)$ *is negligible.*

Non-Slanderability: No PPT adversary can forge a signature that links to one generated by an uncorrupted user. In the non-slanderable game SigSlander, the adversary $\mathcal{A}$ interacts with the challenger $\mathcal{C}$ as follows:

- **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and sends pp to $\mathcal{A}$. $\mathcal{A}$ computes the revoke keypair $(\mathsf{pk}_R, \mathsf{sk}_R)$ and sends pk_R to $\mathcal{C}$.
- **Phase 1.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$.
- **Challenge.** $\mathcal{A}$ outputs the tuple $(\mathsf{ID}^*, M^*, \mathsf{event}^*, L^*)$. It is required that $\mathsf{ID}^* \in L^*$ and $\mathcal{A}$ has never issued an $\mathcal{O}_{\mathsf{KeyExt}}$ query for ID^*. $\mathcal{C}$ computes the signature $\sigma^* \leftarrow \mathsf{Sign}(M^*, \mathsf{event}^*, L^*, d_{\mathsf{ID}^*}, \mathsf{pk}_R)$ and returns σ^* to $\mathcal{A}$.
- **Phase 2.** $\mathcal{A}$ continues querying the oracles, subject to the restriction that $\mathcal{A}$ cannot query $\mathcal{O}_{\mathsf{KeyExt}}$ on ID^* or $\mathcal{O}_{\mathsf{Sign}}$ on $(\cdot, \mathsf{event}^*, \cdot, \mathsf{ID}^*)$.
- **Output.** $\mathcal{A}$ outputs the tuple $(\sigma', M', \mathsf{event}^*, L')$. The game outputs 1 if:
  1. $\mathsf{Verify}(\mathsf{event}^*, \mathsf{pk}_R, L', M', \sigma') = 1$;
  2. $\sigma' \neq \sigma^*$, and σ' was not returned by $\mathcal{O}_{\mathsf{Sign}}$;
  3. $\mathsf{Link}(\mathsf{event}^*, \mathsf{pk}_R, L^*, L', M^*, M', \sigma^*, \sigma') = 1$.

Definition 4 (Non-Slanderability). *An* IB-RLRS *scheme is non-slanderable if for any adversary* $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sigslander}}(\lambda)$ *is negligible.*

Revocability: No PPT adversary can produce a valid signature that can evade revocation by an honest RA with non-negligible probability. The game SigRevoke between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ is defined as follows:

- **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and runs $\mathsf{RevokeKeyGen}(\mathsf{pp})$ to generate the revoke key pair $(\mathsf{pk}_R, \mathsf{sk}_R)$. $\mathcal{C}$ then sends pp and pk_R to $\mathcal{A}$.
- **Queries.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$.
- **Forgery.** $\mathcal{A}$ outputs the challenge tuple $(\sigma^*, M^*, \mathsf{event}^*, L^*)$. Let S_{corr} be the set of identities queried to $\mathcal{O}_{\mathsf{KeyExt}}$. The game outputs 1 if:
  1. $\mathsf{Verify}(M^*, \mathsf{event}^*, L^*, \sigma^*, \mathsf{pk}_R) = 1$;
  2. σ^* was not returned by $\mathcal{O}_{\mathsf{Sign}}$ involving the tuple $(M^*, \mathsf{event}^*, L^*)$;
  3. $\mathcal{A}$ has never query $\mathcal{O}_{\mathsf{Sign}}$ on $(M^*, \mathsf{event}^*, L^*, \mathsf{ID})$ for any uncorrupted identity $\mathsf{ID} \in L^* \setminus S_{corr}$;
  4. $\mathsf{Revoke}(M^*, \mathsf{event}^*, L^*, \sigma^*, \mathsf{sk}_R) \notin (L^* \cap S_{corr})$.

The advantage of $\mathcal{A}$ in winning the game SigRevoke is defined as:

$$\mathsf{Adv}^{\mathsf{sigrevoke}}_{\mathcal{A}}(\lambda) = \Pr[\mathsf{SigRevoke}^{\mathsf{IB\text{-}RLRS}}_{\mathcal{A}}(\lambda) = 1].$$

Definition 5 (Revocability). *An* IB-RLRS *scheme is revocable if for any adversary* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{sigrevoke}}_{\mathcal{A}}(\lambda)$ *is negligible.*

Revocation Soundness: No PPT malicious RA can falsely trace an honest user's valid signature to an incorrect identity associated with a valid proof. The RevSound game between a malicious RA $\mathcal{A}$ and a challenger $\mathcal{C}$ proceeds as follows:

- **Setup.** $\mathcal{C}$ runs $\mathsf{Setup}(\lambda)$ to generate $(\mathsf{pp}, \mathsf{msk})$, and sends pp to $\mathcal{A}$. $\mathcal{A}$ computes its own revoke key pair $(\mathsf{pk}_R, \mathsf{sk}_R)$ and sends pk_R to $\mathcal{C}$.
- **Query.** $\mathcal{C}$ initializes empty lists $\mathcal{Q}_{\mathsf{H}}, \mathcal{Q}_{\mathsf{KeyExt}}, \mathcal{Q}_{\mathsf{Sign}}$ to track $\mathcal{A}$'s adaptive queries to oracles $\mathcal{O}_{\mathsf{H}}, \mathcal{O}_{\mathsf{KeyExt}}, \mathcal{O}_{\mathsf{Sign}}$.
- **Forgery.** $\mathcal{A}$ outputs a slandered target identity ID^*, along with a tuple $(L^*, M^*, \mathsf{event}^*, \sigma^*)$, and a proof π^*_{dec}. Notably, σ^* is allowed to be an output generated by $\mathcal{O}_{\mathsf{Sign}}$. The game RevSound outputs 1 if:
  1. $\mathsf{Verify}(M^*, \mathsf{event}^*, L^*, \sigma^*, \mathsf{pk}_R) = 1$;
  2. $\mathsf{Judge}(M^*, \mathsf{event}^*, L^*, \sigma^*, \mathsf{ID}^*, \pi^*_{dec}, \mathsf{pk}_R) = 1$;
  3. $\mathsf{ID}^* \in L^*$, and $\mathcal{A}$ has never query $\mathcal{O}_{\mathsf{KeyExt}}$ on ID^*;
  4. $\mathcal{A}$ has never issued an $\mathcal{O}_{\mathsf{Sign}}$ query on the tuple $(M^*, \mathsf{event}^*, L^*, \mathsf{ID}^*)$.

The advantage of $\mathcal{A}$ in winning the game RevSound is defined as:

$$\mathsf{Adv}^{\mathsf{revsound}}_{\mathcal{A}}(\lambda) = \Pr[\mathsf{RevSound}^{\mathsf{IB\text{-}RLRS}}_{\mathcal{A}}(\lambda) = 1].$$

Definition 6 (Revocation Soundness). *An* IB-RLRS *scheme satisfies revocation soundness if for any adversary* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{revokesound}}_{\mathcal{A}}(\lambda)$ *is negligible.*

4 Efficient Construction with Logarithmic Signature Size

4.1 Technical Overview

We present a concrete instantiation of our scheme, named BLMQ-RLRS, by integrating the IEEE P1363 signature scheme, Bulletproofs membership proof, Twisted ElGamal public-key encryption, and Chaum-Pedersen protocol as the core building blocks. Our proposed scheme is motivated from [18, 4, 22].

Let $L = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$ be the ring of identities, and let the signer's identity be $\mathsf{ID}_\pi, \pi \in [n]$. To generate a ring signature, the signer must prove that (i)The signer holds a valid private key d_{ID_π} issued by the KGC, and (ii) $\mathsf{ID}_\pi \in L$. To do so, the signer compute the commitment $\mathsf{c} = \mathsf{Com}(x_\pi; r_c)$ of her identity hash value x_π, the set $\boldsymbol{Y} = \{g^{x_1}, \ldots, g^{x_n}\}, x_i = \mathsf{H}(\mathsf{ID}_i)$, and utlize the set membeship proof in [22], which provides a logarithmic-size proof to demonstrate that the value $g^{x_\pi} \in \boldsymbol{Y}$ with transparent setup. To ensure the revocability of the signature, the signer encrypts her identity hash value x_π using the RA's public key and generates a ciphertext $\mathsf{ct} = \mathsf{Enc}(x_\pi; r_e)$. Here we adopt the zk-friendly encrypt scheme, the Twisted ElGamal, to archive revocability with minimum

communication cost. We also adopt the linking tag construction from [17] by defining a deterministic mapping $\mathsf{Tag} : \mathbb{G}_1 \times \{0,1\}^* \to \mathbb{G}_T$, which derives a unique tag from the signer's private key and the event description. Finally, the signatures of knowledges are constructed as follows:

$$\mathcal{R}_{\mathsf{BLMQ\text{-}RLRS}} = \left\{ \begin{matrix} x_\pi, d_{\mathsf{ID}_\pi}, \\ r_c, r_e \end{matrix} \middle| \begin{matrix} g_1^{x_\pi} \in \boldsymbol{Y} \wedge \mathsf{c} \leftarrow \mathsf{Com}(x_\pi; r_c) \wedge \mathsf{ct} \leftarrow \mathsf{Enc}(x_\pi; r_e) \wedge \\ e(d_{\mathsf{ID}_\pi}, g_2^{x_\pi} P_{\mathsf{pub}}) = e(g_1, g_2) \wedge I = \mathsf{Tag}(d_{\mathsf{ID}_\pi}, \mathsf{event}) \end{matrix} \right\}.$$

In our construction, the revocation mechanism is carefully designed to guarantee both revocability and revocation soundness. Assuming that during signature generation, the signer embeds a tracing ciphertext $\mathsf{ct} = (A_0, A_1)$ that encapsulates their identity information $M = g_1^{\mathsf{H}_1(\mathsf{ID}_\pi)}$ under the RA's public key $\mathsf{pk}_R = h^{d_R}$. Upon a revocation request, the RA can leverage the d_R to decrypt this component, recover M, and match it against the ring L to deanonymize the signer. However, simply outputting the identity ID_π is insufficient: an actively malicious RA could falsely accuse an honest, non-participating ring member. To thwart such framing attacks, our framework mandates the RA to produce a revocation proof π_{dec} alongside the extracted identity. Specifically, by defining $B = A_1/M$, a correct decryption implies the discrete logarithm equality $\log_h \mathsf{pk}_R = \log_B A_0 = d_R$. The RA proves this structural relation using a non-interactive Fiat-Shamir transformed Chaum-Pedersen protocol [8]. Consequently, any third party can verify the integrity of the RA's decision via the Judge algorithm, ensuring robust revocability without leaking the RA's secret key. It is recommended to employ a distributed key generation mechanism to mitigate centralized risk by distributing the trust of the KGC and the RA across multiple independent nodes.

4.2 Construction

- $\mathsf{Setup}(\lambda)$: On input a security parameter λ:
  1. Select a pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where the order of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ is q. Select two random generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$. Sample $\mathsf{msk} = s \leftarrow\$ \mathbb{Z}_q^*$ and compute $\mathsf{mpk} = P_{\mathsf{pub}} = g_2^s$. Select cryptographic hash functions $\mathsf{H}_j : \{0,1\}^* \to \mathbb{Z}_q^*$ for $j = 1, \ldots, 6$ and $\mathsf{H}_7 : \{0,1\}^* \to \mathbb{G}_2$.
  2. Let N denote the maximum number of members supported in a single signature. Select mutually independent generators $h, \{h_i\}_{i=1}^N \in \mathbb{G}_1$. The vector $\boldsymbol{h}$ is defined as $\boldsymbol{h} = (h_1, \ldots, h_n)$, consisting of the first n elements from the set $\{h_i\}_{i=1}^N$.
  3. The public parameters are defined as

$$\mathsf{pp} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, g_1, g_2, N, h, \{h_i\}_{i=1}^N, P_{\mathsf{pub}}, \mathsf{H}_1, \ldots, \mathsf{H}_7).$$

- $\mathsf{RevokeKeyGen}(\mathsf{pp})$: The RA samples $\mathsf{sk}_R = d_R \leftarrow\$ \mathbb{Z}_q^*$ and computes the corresponding public key $\mathsf{pk}_R = h^{d_R}$.
- $\mathsf{KeyExt}(\mathsf{ID}, \mathsf{msk})$: For an identity $\mathsf{ID} \in \{0,1\}^*$, the KGC computes $x = \mathsf{H}_1(\mathsf{ID}), t = (s + x)^{-1} \pmod q$ and derives the private key as $d_{\mathsf{ID}} = g_1^t$.

– $\mathsf{Sign}(\mathsf{event}, \mathsf{pk}_R, d_{\mathsf{ID}}, L, m)$: Let $\pi \in [n]$ denote the signer's index in the ring $L = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\}$. Given the $\mathsf{event} \in \{0,1\}^*$, the pk_R, and the message m, the signer with private key d_{ID_π} generates a ring signature σ as follows:
  1. Compute $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$, where $Y_i = g_1^{x_i}$ and $x_i = \mathsf{H}_1(\mathsf{ID}_i) \in \mathbb{Z}_q^*$ for $i \in [n]$. Let $U = \mathsf{H}_7(\mathsf{event})$ and compute the linking tag $I = e(d_{\mathsf{ID}_\pi}, U)$.
  2. Define $\boldsymbol{b}_L \in \{0,1\}^n$ as the one-hot vector with 1 at index π, and let $\boldsymbol{b_R} = \boldsymbol{b_L} - \mathbf{1}^n$. Then, sample $r_2 \leftarrow\!\$\, \mathbb{Z}_q^*$ and compute $A_2 = d_{\mathsf{ID}_\pi} h^{r_2}$, and transform the relation $\mathcal{R}_{\mathsf{BLMQ\text{-}RLRS}}$ into

$$\mathcal{R}' := \left\{ \begin{array}{c} x_\pi, d_{\mathsf{ID}_\pi}, \\ \boldsymbol{b_L}, \boldsymbol{b_R}, \\ r_1, r_2, \end{array} \middle| \begin{array}{c} \boldsymbol{b_L} \circ \boldsymbol{b_R} = \mathbf{0}^n \wedge \boldsymbol{b_L} - \boldsymbol{b_R} = \mathbf{1}^n \wedge \langle \boldsymbol{b_L}, \mathbf{1}^n \rangle = 1 \wedge \\ A_0 = \mathsf{pk}_R^{r_1} \wedge A_1 = \boldsymbol{Y}^{\boldsymbol{b_L}} h^{r_1} \wedge A_2 = d_{\mathsf{ID}_\pi} h^{r_2} \wedge \\ e(d_{\mathsf{ID}_\pi}, g_2^{x_\pi} P_{\mathsf{pub}}) = e(g_1, g_2) \wedge I = e(d_{\mathsf{ID}_\pi}, U) \end{array} \right\}.$$

  3. Sample $r_3, r_4 \leftarrow\!\$\, \mathbb{Z}_q^*$, compute $A_3 = g_1^{r_2} h^{r_3}, A_4 = \boldsymbol{h}^{\boldsymbol{b_R}} h^{r_4}$;
  4. Sample $k_1, k_2, k_3, k_4, k_5, k_6, k_7 \leftarrow\!\$\, \mathbb{Z}_q^*$ and $\boldsymbol{s_L}, \boldsymbol{s_R} \leftarrow\!\$\, \mathbb{Z}_q^n$, and compute

$$S_0 = \mathsf{pk}_R^{k_1}, S_1 = g_1^{k_6} h^{k_1}, S_2 = g_1^{k_2} h^{k_3}, S_3 = g_1^{k_4} h^{k_5} A_3^{-k_6}, S_4 = \boldsymbol{Y}^{\boldsymbol{s_L}} \boldsymbol{h}^{\boldsymbol{s_R}} h^{k_7},$$
$$S_5 = e(A_2, g_2)^{k_6} e(h, g_2)^{-k_4} e(h, P_{\mathsf{pub}})^{-k_2}, S_6 = e(h, U)^{k_2}.$$

  5. Let $\mathsf{str} = \boldsymbol{Y} \| A_0 \| A_1 \| A_2 \| A_3 \| A_4 \| I \| S_0 \| S_1 \| S_2 \| S_3 \| S_4 \| S_5 \| S_6 \| U \| m \| \mathsf{event}$, compute $y = \mathsf{H}_3(\mathsf{str}), z = \mathsf{H}_4(\mathsf{str}), w = \mathsf{H}_5(\mathsf{str})$ and $\boldsymbol{y}^n = (1, y, \ldots, y^{n-1})$.
  6. Compute $l(X) = \boldsymbol{b_L} - z \cdot \mathbf{1}^n + \boldsymbol{s_L} \cdot X$ and $r(X) = \boldsymbol{y}^n \circ (w \cdot \boldsymbol{b_R} + wz \cdot \mathbf{1}^n + \boldsymbol{s_R} X) + z^2 \cdot \mathbf{1}^n$. Denote $t(X) = \langle l(X), r(X) \rangle = t_0 + t_1 X + t_2 X^2$, where

$$\begin{aligned} t_0 &= z^2 + w(z - z^2)\langle \mathbf{1}^n, \boldsymbol{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle \\ t_1 &= \langle \boldsymbol{b_L} - z\mathbf{1}^n, \boldsymbol{s_R} \circ \boldsymbol{y}^n \rangle + w\langle \boldsymbol{s_L}, \boldsymbol{y}^n \circ \boldsymbol{b_R} \rangle + wz\langle \boldsymbol{s_L}, \boldsymbol{y}^n \rangle + z^2 \langle \boldsymbol{s_L}, \mathbf{1}^n \rangle \\ t_2 &= \langle \boldsymbol{s_L}, \boldsymbol{s_R} \circ \boldsymbol{y}^n \rangle \end{aligned}$$

  7. Sample $\tau_1, \tau_2 \leftarrow \mathbb{Z}_q$ and Compute $T_i = g_1^{t_i} h^{\tau_i}$ for $i \in \{1, 2\}$.
  8. Compute the challenge $x = \mathsf{H}_2(y \| z \| w \| T_1 \| T_2 \| m \| \mathsf{event})$, and compute the responses

$$\begin{aligned} \boldsymbol{l} &= l(x) = \boldsymbol{b_L} - z \cdot \mathbf{1}^n + \boldsymbol{s_L} \cdot x, \\ \boldsymbol{r} &= r(x) = \boldsymbol{y}^n \circ (w \cdot \boldsymbol{b_R} + wz \cdot \mathbf{1}^n + \boldsymbol{s_R} \cdot x) + z^2 \cdot \mathbf{1}^n, \end{aligned}$$

$$\begin{aligned} &\tau_x = \tau_1 \cdot x + \tau_2 \cdot x^2, \quad && s_1 = k_1 + x \cdot r_1, && s_2 = k_2 + x \cdot r_2, \\ &s_3 = k_3 + x \cdot r_3, && s_4 = k_4 + x \cdot r_2 x_\pi, && s_5 = k_5 + x \cdot r_3 x_\pi, \\ &s_6 = k_6 + x \cdot x_\pi, && s_7 = r_1 + w r_4 + k_7 \cdot x, && t = \langle \boldsymbol{l}, \boldsymbol{r} \rangle. \end{aligned}$$

  Outputs $\sigma = (A_0, \ldots, A_4, I, S_0, \ldots, S_6, T_1, T_2, \tau_x, \boldsymbol{l}, \boldsymbol{r}, s_1, \ldots, s_7, t)$ as a signature on event, pk_R, L, and m.
– $\mathsf{Verify}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma)$: The verifier first checks whether $\mathsf{pk}_R \neq 1_{\mathbb{G}_1}$ holds. If not, the verifier rejects. Then, the verifier computes $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$ where $Y_i = g_1^{x_i}$ and $x_i = \mathsf{H}_1(\mathsf{ID}_i)$ for $i \in [n]$, and $U = \mathsf{H}_7(\mathsf{event})$, verifies the signature σ as follows:

1. Let $\mathsf{str} = \boldsymbol{Y}\|A_0\|A_1\|A_2\|A_3\|A_4\|I\|S_0\|S_1\|S_2\|S_3\|S_4\|S_5\|S_6\|U\|m\|\mathsf{event}$, compute $y = \mathsf{H}_3(\mathsf{str}), z = \mathsf{H}_4(\mathsf{str}), w = \mathsf{H}_5(\mathsf{str})$, $\boldsymbol{y}^n = (1, y, \ldots, y^{n-1})$, and $\boldsymbol{h'} = (h'_1, \ldots, h'_n) = (h_1, h_2^{y^{-1}}, \ldots, h_n^{y^{-n+1}})$.
2. Check the following equations:

$$t = \langle \boldsymbol{l}, \boldsymbol{r} \rangle, \tag{1}$$

$$g_1^t h^{\tau_x} = g_1^{z^2 + w(z - z^2)\langle \mathbf{1}^n, \boldsymbol{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle} T_1^x \cdot T_2^{x^2}, \tag{2}$$

$$\boldsymbol{Y}^{\boldsymbol{l}} \boldsymbol{h'}^{\boldsymbol{r}} h^{s_7} = A_1 A_4^w S_4^x \boldsymbol{Y}^{-z\mathbf{1}^n} \boldsymbol{h'}^{wz\boldsymbol{y}^n + z^2 \mathbf{1}^n}, \tag{3}$$

$$\mathsf{pk}_R^{s_1} = S_0 A_0^x, \tag{4}$$

$$g_1^{s_6} h^{s_1} = S_1 A_1^x, \tag{5}$$

$$g_1^{s_2} h^{s_3} = S_2 A_3^x, \tag{6}$$

$$g_1^{s_4} h^{s_5} A_3^{-s_6} = S_3, \tag{7}$$

$$e(A_2^{s_6} h^{-s_4}, g_2) e(h^{-s_2}, P_{\mathsf{pub}}) = S_5 \cdot (e(g_1, g_2) e(A_2^{-1}, P_{\mathsf{pub}}))^x, \tag{8}$$

$$e(h, U)^{s_2} = S_6 \cdot e(A_2, U)^x I^{-x}. \tag{9}$$

   The verifier outputs 1 if and only if all aforementioned equations hold; otherwise, it outputs 0.

– $\mathsf{Link}(\mathsf{event}, \mathsf{pk}_{R1}, \mathsf{pk}_{R2}, L_1, L_2, m_1, m_2, \sigma_1, \sigma_2)$: The algorithm verifies σ_1 and σ_2; if either is invalid, it returns 0. Then, it outputs 1 if $I_1 = I_2$, and 0 otherwise.
– $\mathsf{Revoke}(\mathsf{event}, \mathsf{sk}_R, L, m, \sigma)$: For a revocation request, the RA runs as follows:
  1. Verify the validity of the signature σ. If invalid, output $\perp$.
  2. Compute $u = -d_R^{-1} \pmod q$ and $M = A_1 \cdot A_0^u = g_1^{x_\pi}$.
  3. Find $\mathsf{ID} \in L$ s.t. $g_1^{\mathsf{H}_1(\mathsf{ID})} = M$. Return ID if found; otherwise, output $\perp$.
  4. Let $B = A_1/M$. To generate the revocation proof π_{dec}, sample $r \leftarrow\!\!\$\, \mathbb{Z}_q$, and compute $(C_0, C_1) = (h^r, B^r)$.
  5. Compute the Fiat-Shamir challenge $c = \mathsf{H}_6(\mathsf{pk}_R\|A_0\|B\|C_0\|C_1)$.
  6. Compute the response $z = r + c \cdot d_R \pmod q$.
  7. Output the extracted identity and the proof as $(\mathsf{ID}, \pi_{dec} = (C_0, C_1, z))$.
– $\mathsf{Judge}(\mathsf{event}, \mathsf{pk}_R, L, m, \sigma, \mathsf{ID}, \pi_{dec})$: On input a judge request, the algorithm first verifies the validity of the signature σ. If σ is invalid, it rejects. Otherwise, compute $x_\pi = \mathsf{H}_1(\mathsf{ID})$ and $B = A_1/g_1^{x_\pi}$. Then compute the challenge $c = \mathsf{H}_6(\mathsf{pk}_R\|A_0\|B\|C_0\|C_1)$, checks whether the equations $h^{z_{d_R}} = C_0 \cdot \mathsf{pk}_R^c$ and $B^{z_{d_R}} = C_1 \cdot A_0^c$ holds. If both equations hold, the judge accepts; otherwise, it rejects

By applying the work of [6], two vectors $\boldsymbol{l}, \boldsymbol{r}$ with size n could be compressed into two vectors $\boldsymbol{L'}, \boldsymbol{R'}$ with size $\log n$, along with two elements $a, b \in \mathbb{Z}_p$, thus achieving logarithmic signature size. Further details can be found in [6].

4.3 Comparison

The communication costs of our scheme and [17] are shown in the table below, which also achieves logarithmic signature size. We employ a 256-bit BN curve and adapt [17] to the asymmetric bilinear pairing setting for a fair comparison.

Table 1. Communication Comparsion.

Ring Size	2	4	8	16	32	64	128	256	512	1024	2048
[17]	9728	15616	21504	27392	33280	39168	45056	50944	56832	62720	68608
IB-RLRS	19200	20224	21248	22272	23296	24320	25344	26368	27392	28416	29440

5 Security Proofs

Theorem 1. *Under the DL assumption in $\mathbb{G}_1$, the relation $\mathcal{R}'$ presented in the* Sign *algorithm is a signature of knowledge satisfying completeness, soundness, and zero-knowledge in the random oracle model.*

Proof. **Completeness.** The completeness property is straightforward and is therefore omitted. We refer the reader to [22, 18] for further details.

Soundness. If there exists a PPT adversary $\mathcal{A}$ that can produce a valid signature σ for a message m, an event event, and ring L without knowing the witness for the relation $\mathcal{R}'$, then we can construct a PPT extractor $\mathcal{E}$ that can extract a valid witness $(x_\pi, d_{\mathsf{ID}_\pi}, \boldsymbol{b_L}, \boldsymbol{b_R}, r_1, r_2)$ by interacting with $\mathcal{A}$.

Using rewinding techniques [22], $\mathcal{E}$ rewinds $\mathcal{A}$ to the oracle $\mathcal{O}_{\mathsf{H}_2}$ for three times to obtain three distinct transcripts $\mathsf{trans}_i = \{x_i, (\tau_{x,i}, \boldsymbol{l}_i, \boldsymbol{r}_i, t_i, s_{1,i}, \ldots, s_{7,i})\}$ for $i \in \{1, 2, 3\}$, where the challenges satisfy $x_i \neq x_j$ for all $i \neq j$. Since the rewinding is performed exclusively on $\mathcal{O}_{\mathsf{H}_2}$, the challenges y, z, and w can be computed independently by $\mathcal{E}$ and remain invariant across all retrieved transcripts.

Let $\zeta = r_1 + wr_4$, thus $A_1 A_4^w = \boldsymbol{Y}^{\boldsymbol{b_L}} \boldsymbol{h}^{w\boldsymbol{b_R}} h^\zeta$. To extract $(\boldsymbol{b_L}, \boldsymbol{b_R}, \zeta)$, $\mathcal{E}$ computes coefficients η_1, η_2 satisfying $\sum_{i=1}^2 \eta_i = 1$ and $\sum_{i=1}^2 \eta_i x_i = 0$. By combining the equation (3) with η_i, $\mathcal{E}$ eliminates S_4 and reconstructs the witness as:

$$\boldsymbol{b'_L} = \sum_{i=1}^{2} \eta_i \boldsymbol{l}_i + z\mathbf{1}^n, \boldsymbol{b'_R} = w^{-1}[(\sum_{i=1}^{2} \eta_i \boldsymbol{r}_i - wz\boldsymbol{y}^n - z^2\mathbf{1}^n) \circ \boldsymbol{y}^{-n}], \zeta' = \sum_{i=1}^{2} \eta_i s_{7,i}.$$

To extract $(\boldsymbol{s_L}, \boldsymbol{s_R}, k_7)$, $\mathcal{E}$ computes coefficients θ_1, θ_2 satisfying $\sum_{i=1}^2 \theta_i = 0$ and $\sum_{i=1}^2 \theta_i x_i = 1$. By combining the equation (3) with θ_i, the witness tuple $(\boldsymbol{s'_L}, \boldsymbol{s'_R}, k'_7)$ can be reconstructed as:

$$\boldsymbol{s'_L} = \sum_{i=1}^{2} \theta_i \cdot \boldsymbol{l}_i, \quad \boldsymbol{s'_R} = (\sum_{i=1}^{2} \theta_i \boldsymbol{r}_i) \circ \boldsymbol{y}^{-n}, \quad k'_7 = \sum_{i=1}^{2} s_{7,i}\theta_i.$$

Putting the tuple $(\boldsymbol{b'_L}, \boldsymbol{b'_R}, \zeta', \boldsymbol{s'_L}, \boldsymbol{s'_R}, k'_7)$ back to the equation (3), $\mathcal{A}$'s response can be rewritten as the polynomial $t(X)$ evaluated at the challenge x:

$$\begin{aligned} s_7 &= \zeta' + k'_7 \cdot x, \\ \boldsymbol{l} &= \boldsymbol{b'_L} - z \cdot \mathbf{1}^n + \boldsymbol{s'_L} \cdot x, \\ \boldsymbol{r} &= \boldsymbol{y}^n \circ (w \cdot \boldsymbol{b'_R} + wz \cdot \mathbf{1}^n + \boldsymbol{s'_R} \cdot x) + z^2 \cdot \mathbf{1}^n. \end{aligned}$$

Using the same set of trans, $(t_1', \tau_1', t_2', \tau_2')$ can be efficiently extracted. Specifically, utilizing the invertibility of the Vandermonde matrix defined by the distinct challenges, $\mathcal{E}$ can find a unique coefficient vector $(\delta_1, \delta_2, \delta_3) \in \mathbb{Z}_q^3$ to eliminate the constant and quadratic terms in the verification equations. This yields $T_1 = g_1^{t_1'} h^{\tau_1'}$, where $t_1' = \sum_{i=1}^3 \delta_i t_i$ and $\tau_1' = \sum_{i=1}^3 \delta_i \tau_{x,i}$. Similarly, to extract T_2, the $\mathcal{E}$ choose another unique vector $(\delta_1', \delta_2', \delta_3') \in \mathbb{Z}_q^3$ satisfying $\sum_{i=1}^3 \delta_i' = 0$, $\sum_{i=1}^3 \delta_i' x_i = 0$, and $\sum_{i=1}^3 \delta_i' x_i^2 = 1$. This yields $T_2 = g_1^{t_2'} h^{\tau_2'}$, where $t_2' = \sum_{i=1}^3 \delta_i' t_i$ and $\tau_2' = \sum_{i=1}^3 \delta_i' \tau_{x,i}$.

Putting $(t_1', \tau_1', t_2', \tau_2')$ back into the equation (2), we have:

$$g_1^t h^{\tau_x} = g_1^{z^2 + w(z-z^2)\langle \mathbf{1}^n, \boldsymbol{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle} \cdot (g_1^{t_1'} h^{\tau_1'})^x \cdot (g_1^{t_2'} h^{\tau_2'})^{x^2}.$$

Since the DL assumption holds in $\mathbb{G}_1$, $\log_{g_1} h$ is unknown to $\mathcal{A}$ and cannot be computed. Therefore, we have $t = z^2 + w(z-z^2)\langle \mathbf{1}^n, \boldsymbol{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle + t_1' x + t_2' x^2$. On the other hand, since $t = \langle \boldsymbol{l}, \boldsymbol{r} \rangle$, we have: $\exists t_1'', t_2''$, such that:

$$\begin{aligned}
\langle \boldsymbol{l}, \boldsymbol{r} \rangle &= \langle \boldsymbol{b_L'} - z \cdot \mathbf{1}^n + \boldsymbol{s_L'} \cdot x, \boldsymbol{y}^n \circ (w \cdot \boldsymbol{b_R'} + wz \cdot \mathbf{1}^n + \boldsymbol{s_R'} \cdot x) + z^2 \cdot \mathbf{1}^n \rangle, \\
&= w \langle \boldsymbol{b_L'}, \boldsymbol{b_R'} \circ \boldsymbol{y}^n \rangle + wz \langle \boldsymbol{b_L'} - \boldsymbol{b_R'}, \boldsymbol{y}^n \rangle + z^2 \langle \boldsymbol{b_L'}, \mathbf{1}^n \rangle - wz^2 \langle \mathbf{1}^n, \boldsymbol{y}^n \rangle \\
&\quad - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle + t_1'' x + t_2'' x^2, \\
t_1'' &= \langle \boldsymbol{b_L'} - z\mathbf{1}^n, \boldsymbol{s_R'} \circ \boldsymbol{y}^n \rangle + w \langle \boldsymbol{s_L'}, \boldsymbol{y}^n \circ \boldsymbol{b_R'} \rangle + wz \langle \boldsymbol{s_L'}, \boldsymbol{y}^n \rangle + z^2 \langle \boldsymbol{s_L'}, \mathbf{1}^n \rangle, \\
t_2'' &= \langle \boldsymbol{s_L'}, \boldsymbol{s_R'} \circ \boldsymbol{y}^n \rangle.
\end{aligned}$$

Note that the algebraic structures of the extracted coefficients t_1'' and t_2'' are identical to t_1 and t_2 computed in the Sign algorithm. Since the challenges (w, x, y, z) are independently and uniformly sampled in the random oracle model, the verification equation holds with a non-negligible probability if and only if the corresponding coefficients on both sides match identically. This implies that:

$$\boldsymbol{b_L}' \circ \boldsymbol{b_R}' = \mathbf{0}^n, \quad \boldsymbol{b_L}' - \boldsymbol{b_R}' = \mathbf{1}^n, \quad \langle \boldsymbol{b_L}', \mathbf{1}^n \rangle = 1,$$

which forces $\boldsymbol{b_L}'$ to be a valid one-hot vector. Consequently, by substituting this into equation (3), there must exist a unique index π^* such that $A_1 A_4^w = Y_{\pi^*} \boldsymbol{h}^{w\boldsymbol{b_R}'} h^{\zeta'} = g_1^{x_\pi'} \boldsymbol{h}^{w\boldsymbol{b_R}'} h^{r_1' + wr_4'}$. On the other hand, since A_1 is generated prior to and independent of the challenge w, by equating the constant terms with respect to w on both sides, we successfully isolate $A_1 = g_1^{x_\pi'} h^{r_1'}$.

To extract d_{ID_π}, observe the response relations $s_{2,1} = k_2 + x_1 r_2$ and $s_{2,2} = k_2 + x_2 r_2$ from the transcripts, which allows $\mathcal{E}$ to compute $r_2' = (s_{2,1} - s_{2,2})/(x_1 - x_2)$. The private key can then be extracted via $d_{\mathsf{ID}_\pi}' = A_2 h^{-r_2'}$.

Next, we substitute the two trans into the verification equation (8). By dividing the two resulting relations, we obtain the eliminated pairing equation:

$$e(A_2, g_2)^{\Delta s_6} \cdot e(h, P_{pub}^{-\Delta s_2} g_2^{-\Delta s_4}) = e(g_1 A_2^{-1}, P_{pub})^{\Delta x},$$

where $\Delta x = x_2 - x_1$ and $\Delta s_i = s_{i,2} - s_{i,1}$. By substituting $A_2 = d_{\mathsf{ID}_\pi}' h^{r_2'}$ into the above relation, we have $e(d_{\mathsf{ID}_\pi'}, g_2^{x_\pi'} P_{pub}) = e(g_1, g_2)$, meaning that $(x_\pi', d_{\mathsf{ID}_\pi}')$

satisfies the key generation relation. Consequently, $\mathcal{E}$ successfully reconstructs the witness $(x_\pi, d_{\mathsf{ID}_\pi}, \boldsymbol{b_L}, \boldsymbol{b_R}, r_1, r_2)$, which completes the proof of soundness.

Zero-Knowledge. The simulator $\mathcal{S}$ samples challenges $x, y, z, w \leftarrow\!\$\ \mathbb{Z}_q^*$, responses $\tau_x, s_1, \ldots, s_7 \leftarrow\!\$\ \mathbb{Z}_q^*, \boldsymbol{l}, \boldsymbol{r} \leftarrow\!\$\ \mathbb{Z}_q^n$, and $A_0, \ldots, A_4, T_1 \leftarrow\!\$\ \mathbb{G}_1, I \in \mathbb{G}_T$, computes $t = \langle \boldsymbol{l}, \boldsymbol{r} \rangle$ and

$$
\begin{aligned}
T_2 &= (g_1^t h^{\tau_x} g_1^{-(z^2 + w(z-z^2)\langle \mathbf{1}^n, \boldsymbol{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{1}^n \rangle)} T_1^{-x})^{x^{-2}}, \\
S_0 &= \mathsf{pk}_A^{s_1} A_0^{-x}, \quad S_1 = g_1^{s_6} h^{s_1} A_1^{-x}, \\
S_2 &= g_1^{s_2} h^{s_3} A_3^{-x}, \quad S_3 = g_1^{s_4} h^{s_5} A_3^{-s_6}, \\
S_4 &= (\boldsymbol{Y}^{\boldsymbol{l} + z\mathbf{1}^n} \boldsymbol{h'}^{\boldsymbol{r} - wz \cdot \boldsymbol{y}^n - z^2 \cdot \mathbf{1}^n} A_1^{-1} \cdot A_4^{-w} h^{s_7})^{x^{-1}}, \\
S_5 &= e(A_2^{s_6} h^{-s_4}, g_2) e(h^{-s_2}, P_{pub}) \cdot (e(g_1, g_2) e(A_2^{-1}, P_{pub}))^{-x}, \\
S_6 &= e(h, U)^{s_2} e(A_2, U)^{-x} I^x.
\end{aligned}
$$

Then $\mathcal{S}$ programs the $\mathcal{O}_{\mathsf{H}_2}, \ldots, \mathcal{O}_{\mathsf{H}_5}$ according to the Sign algorithm to output the pre-selected challenges (x, y, z, w), and finally outputs the simulated signature $\sigma = (A_0, \ldots, A_4, I, S_0, \ldots, S_6, T_1, T_2, \tau_x, s_1, \ldots, s_7, \boldsymbol{l}, \boldsymbol{r}, t)$. Obviously, the simulated distribution is identical to that of a real signature.

Theorem 2 (Unforgeability). *If the q-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$, then our scheme achieves EUF-CMIA security in the random oracle model.*

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ breaking the EUF-CMIA security with non-negligible probability ϵ. We construct a simulator $\mathcal{B}$ to solve the q-SDH instance $(g_1, g_2, g_2^s, \ldots, g_2^{s^q})$. We assume $\mathcal{A}$ makes at most $q_{\mathsf{H}_1} \leq q$ queries to $\mathcal{O}_{\mathsf{H}_1}$, and the number of queries to other oracles is bounded by $\mathsf{poly}(\lambda)$.

Setup. $\mathcal{B}$ guesses the index $k^* \leftarrow\!\$\ [1, q_{\mathsf{H}_1}]$ for the forged identity and samples $\alpha_1, \ldots, \alpha_{q-1} \leftarrow\!\$\ \mathbb{Z}_q^* \setminus \{\alpha^*\}$. Following the standard reduction technique [1], $\mathcal{B}$ implicitly defines the polynomial $f(x) = \prod_{i=1}^{q-1}(\alpha_i + x)$ and leverages the q-SDH instance to compute the system generators as $G_2 = g_2^{f(s)}$ and $G_1 = g_1^{f(s)}$. The master public key is set to $P_{\mathsf{pub}} = G_2^s = g_2^{s \cdot f(s)}$. $\mathcal{B}$ then initializes the remaining parameters honestly and sends pp to $\mathcal{A}$.

Oracle Queries. $\mathcal{B}$ maintains initially empty lists $\mathcal{Q}_{\mathsf{H}_1}, \ldots, \mathcal{Q}_{\mathsf{H}_7}$, $\mathcal{Q}_{\mathsf{KeyExt}}$ and $\mathcal{Q}_{\mathsf{Sign}}$, answers the queries as follows:

- $\mathcal{O}_{\mathsf{H}_1}(\mathsf{ID})$**:** If ID exists in $\mathcal{Q}_{\mathsf{H}_1}$, return the previously recorded value. If this is the k^*-th query, $\mathcal{B}$ sets $\mathsf{H}_1(\mathsf{ID}) = \alpha^*$ and records $(\mathsf{ID}, \alpha^*, \perp)$. Otherwise, $\mathcal{B}$ returns an unused value $\alpha_i \in \{\alpha_1, \ldots, \alpha_{q-1}\}$, and records $(\mathsf{ID}, \alpha_i, i)$.
- $\mathcal{O}_{\mathsf{KeyExt}}(\mathsf{ID})$**:** $\mathcal{B}$ queries $x = \mathsf{H}_1(\mathsf{ID})$. If $x = \alpha^*$, $\mathcal{B}$ aborts the simulation. Otherwise, $x = \alpha_i$ for some $i \in [1, q-1]$, and $\mathcal{B}$ computes the valid private key $d_{\mathsf{ID}} = g_1^{f(s)/(s+\alpha_i)}$ directly from the q-SDH instance via polynomial division.
- $\mathcal{O}_{\mathsf{Sign}}(M, \mathsf{event}, L, \mathsf{ID}_\pi)$**:** If $\mathsf{ID}_\pi \neq \mathsf{ID}_{k^*}$, $\mathcal{B}$ extracts the private key and generates the signature honestly. If $\mathsf{ID}_\pi = \mathsf{ID}_{k^*}$, $\mathcal{B}$ leverages the zero-knowledge simulator to produce a valid simulated signature, appropriately programming the random oracles to ensure verification consistency.

Forgery and Extraction. Eventually, $\mathcal{A}$ outputs a valid forgery tuple $(\mathsf{event}^*, L^*, M^*, \sigma^*)$. By the soundness of the relation $\mathcal{R}'$, $\mathcal{B}$ applies the Forking Lemma to extract a valid witness tuple from σ^*, including the signer's identity hash x_π and the private key d^*. If $x_\pi \neq \alpha^*$, $\mathcal{B}$ aborts. Otherwise, the extracted private key satisfies $d^* = g_1^{f(s)/(s+\alpha^*)}$. Since $f(-\alpha^*) \neq 0$, $\mathcal{B}$ performs standard polynomial division $f(x) = Q(x)(x+\alpha^*) + R$ with $R \neq 0$ to efficiently compute $W = g_1^{Q(s)}$ from the given q-SDH instance. $\mathcal{B}$ then isolates the target value as $Z = (d^*/W)^{R^{-1} \pmod q} = g_1^{1/(s+\alpha^*)}$. The pair (α^*, Z) trivially solves the q-SDH instance, contradicting the underlying assumption and demonstrating that $\mathcal{A}$'s advantage ϵ must be negligible.

Probability Analysis. $\mathcal{B}$ completes the simulation without aborting if it correctly guesses the target identity, occurring with probability $1/q_{\mathsf{H}_1}$. Conditioned on this, applying the Forking Lemma yields $\mathcal{B}$'s total advantage in solving the q-SDH problem as $\epsilon' \geq \frac{1}{q_{\mathsf{H}_1}}\epsilon\left(\frac{\epsilon}{q_{\mathsf{H}_2}} - \frac{1}{q}\right)$. Since the q-SDH assumption dictates that ϵ' is negligible, $\mathcal{A}$'s forgery advantage ϵ must identically be negligible. □

Theorem 3 (Anonymity). *If the DDH assumption holds in $\mathbb{G}_1$, the q-DBDHI assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$, and the relation $\mathcal{R}'$ satisfies zero-knowledge, then our scheme achieves anonymity in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary that breaks the anonymity of the scheme with non-negligible advantage ϵ. $\mathcal{B}$ simulate the oracle $\mathcal{O}_{\mathsf{Revoke}}(M, \mathsf{event}, L, \sigma)$ by executes $\mathsf{Revoke}(\mathsf{event}, \mathsf{sk}_R, L, m, \sigma)$ and returns (ID, π_{dec}) to $\mathcal{A}$, and simulates the environments via a sequence of games as follows:

Game 0: This is the original anonymity game $\mathsf{SigAnon}$. The advantage of $\mathcal{A}$ in this game is defined as $\Pr[S_0] = \Pr[b' = b]$.

Game 1: $\mathcal{B}$ computes the $A_0, \ldots, A_4$ and I using the private key of the challenge identity ID_{i_b} along with $r_1, r_2, r_3, r_4 \leftarrow\!\$\, \mathbb{Z}_q^*$, and vectors $\boldsymbol{b_L}, \boldsymbol{b_R}$ constructed as in the real scheme. Then $\mathcal{B}$ invokes the zero-knowledge simulator $\mathcal{S}$. It uniformly samples the challenges (x, y, z, w) and the responses $(\tau_x, s_{1\ldots7}, \boldsymbol{l}, \boldsymbol{r}, T_1)$, and programs the oracles to satisfy the verification equations. The simulated signature σ^*_{sim} is then given to $\mathcal{A}$. If $\mathcal{A}$ distinguishes Game 1 from Game 0 with advantage ϵ_{sok}, $\mathcal{B}$ effectively breaks the zero-knowledge property of the relation $\mathcal{R}'$. Given that this property holds, ϵ_{sok} must be negligible. By the Difference Lemma [21], $|\Pr[S_1] - \Pr[S_0]| \leq \epsilon_{\text{sok}}$.

Game 2: $\mathcal{B}$ further modifies the challenge signature by replacing the ciphertext component A_1^* with a uniformly random element $R_1 \leftarrow\!\$\, \mathbb{G}_1$. Distinguishing Game 2 from Game 1 is equivalent to solving the DDH problem in $\mathbb{G}_1$.

Given a DDH tuple $(g, X = g^a, Y = g^b, T)$, $\mathcal{B}$ sets $\mathsf{pk}_R = g$ and $h = X$. During the challenge phase, $\mathcal{B}$ embeds the DDH instance by setting $A_0^* = Y$ (implicitly setting $r_1 = b$) and $A_1^* = g_1^{x_{i_b}} \cdot T$. If $T = g^{ab} = h^{r_1}$, A_1^* matches the honest distribution in Game 1. If T is random, A_1^* is uniformly distributed in $\mathbb{G}_1$, simulating Game 2. Since $\mathcal{B}$ lacks sk_R, it simulates subsequent $\mathcal{O}_{\mathsf{Revoke}}$ queries by extracting the actual signer's identity via the soundness of the relation $\mathcal{R}'$, and generating π_{dec} via the ZK simulator of the Chaum-Pedersen protocol. This yields $|\Pr[S_2] - \Pr[S_1]| \leq \epsilon_{\mathsf{ddh}}$.

Game 3: $\mathcal{B}$ modifies A_2^* in the challenge signature, replacing it with a uniformly random element $R_2 \leftarrow\$ \mathbb{G}_1$. The reduction to the DDH problem is entirely analogous to that in Game 2. Consequently, $|\Pr[S_3] - \Pr[S_2]| \leq \epsilon_{\mathsf{ddh}}$.
Game 4: $\mathcal{B}$ modifies the linking tag in the challenge signature, replacing $I^* = e(d_{\mathsf{ID}_{i_b}}, U^*)$ with a uniformly random element $R_T \leftarrow\$ \mathbb{G}_T$. Distinguishing Game 4 from Game 3 is equivalent to solving the q-DBDHI problem in $(\mathbb{G}_1, \mathbb{G}_2)$. Given an instance $(g_1, g_2, g_2^{\alpha}, \ldots, g_2^{\alpha^q}, T)$ where T is either $e(g_1, g_2)^{1/\alpha}$ or random, $\mathcal{B}$ guesses the target index $k^* \leftarrow\$ [1, q_{\mathsf{H}_1}]$, sets $\alpha^* = H_1(\mathsf{ID}_{k^*})$, and implicitly defines the master secret key as $s = \alpha - \alpha^*$. The parameters $(G_1, G_2, P_{\mathsf{pub}})$ and $f(x)$ are constructed identically to the unforgeability proof. $\mathcal{B}$ simulates $\mathcal{O}_{\mathsf{KeyExt}}$ using the instance. For $\mathcal{O}_{\mathsf{H}_7}$, $\mathcal{B}$ samples $u \leftarrow\$ \mathbb{Z}_q^*$ and returns $U = G_2^u$.

In the challenge phase, $\mathcal{B}$ aborts if $\mathsf{ID}_{i_b} \neq \mathsf{ID}_{k^*}$. Otherwise, the target private key is $d_{\mathsf{ID}_{i_b}} = G_1^{\frac{1}{s+\alpha^*}} = g_1^{\frac{f(s)}{\alpha}}$. Using polynomial division, $f(s) = \alpha Q(s) + R$ where $R = f(-\alpha^*)$, yielding $d_{\mathsf{ID}_{i_b}} = W \cdot g_1^{R/\alpha}$ for a computable $W = g_1^{Q(s)}$. The linking tag expands to:

$$I^* = e(d_{\mathsf{ID}_{i_b}}, U^*) = e(W, G_2)^{u^*} \cdot e(g_1, g_2)^{\frac{R \cdot u^* \cdot f(s)}{\alpha}}.$$

Expanding $f(s) = f(-\alpha^*) + \alpha H(\alpha)$ for some computable polynomial $H(\alpha)$, $\mathcal{B}$ isolates the computable term $K_{known} = e(W, G_2)^{u^*} \cdot e(g_1, g_2)^{R \cdot u^* \cdot H(\alpha)}$ and embeds the challenge T for the fractional term:

$$I^* = K_{known} \cdot T^{R \cdot u^* \cdot f(-\alpha^*)}.$$

If $T = e(g_1, g_2)^{1/\alpha}$, I^* is perfectly formed; if T is random, I^* is uniformly random in $\mathbb{G}_T$. Thus, $|\Pr[S_4] - \Pr[S_3]| \leq q_{H_1} \cdot \epsilon_{\mathsf{dbdhi}}$.

Conclusion: In Game 4, R_1, R_2, and R_T are uniformly distributed, and σ^* is independent of the underlying witness, and hence statistically independent of the challenge bit b, yielding $\Pr[S_4] = 1/2$. Summing the probability bounds across all game transitions, $\mathcal{A}$'s overall advantage is bounded by:

$$\mathsf{Adv}_{\mathcal{A},\mathsf{SigAnon}}(\lambda) \leq \epsilon_{\mathsf{sok}_{\mathsf{zk}}} + 2 \cdot \epsilon_{\mathsf{ddh}} + q_{\mathsf{H}_1} \cdot \epsilon_{\mathsf{dbdhi}}.$$

The total advantage of the adversary is negligible. □

Since the proof of linkability, non-slanderability, revocability, and revocation soundness can be derived from soundness, zero-knowledge, and unforgeability, we defer the proof to the Appendix B.

6 Conclusion

In this paper, we introduced the concept of Identity-Based Revocable Linkable Ring Signatures (IB-RLRS) and presented an efficient construction featuring a logarithmic signature size. A natural direction for future work is to extend the IB-RLRS to the lattice-based setting, thereby achieving post-quantum security.

A Preliminaries

A.1 IEEE P1363 Signature

We adopt the IEEE P1363 identity-based signature scheme [1], which consists of the following four PPT algorithms:

- $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Setup}(\lambda)$: On input a security parameter λ, select a bilinear group $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$. Let $\mathsf{H}_1, \mathsf{H}_2 : \{0,1\}^* \to \mathbb{Z}_q^*$ be cryptographic hash functions. Sample $\mathsf{msk} = s \leftarrow\$ \mathbb{Z}_q^*$ and compute $\mathsf{mpk} = P_{\mathsf{pub}} = g_2^s$, along with $g = e(g_1, g_2)$, output $\mathsf{pp} = (\mathcal{G}, g, \mathsf{H}_1, \mathsf{H}_2, P_{\mathsf{pub}})$, which are provided implicitly to all subsequent algorithms.
- $d_{\mathsf{ID}} \leftarrow \mathsf{KeyExt}(\mathsf{ID}, \mathsf{msk})$: For an identity $\mathsf{ID} \in \{0,1\}^*$, the KGC computes $x = \mathsf{H}_1(\mathsf{ID}), t = (s + x)^{-1} \pmod q$ and derives the private key as $d_{\mathsf{ID}} = g_1^t$.
- $\sigma \leftarrow \mathsf{Sign}(m, d_{\mathsf{ID}})$: Sample $r \leftarrow\$ \mathbb{Z}_q^*$ and compute $R = g^r$. Set $h = \mathsf{H}_2(m \parallel R)$ and $S = d_{\mathsf{ID}}^{r+h}$. Output $\sigma = (h, S)$.
- $b \leftarrow \mathsf{Verify}(m, \sigma, \mathsf{ID})$: Parse $\sigma = (h, S)$. Compute $x = \mathsf{H}_1(\mathsf{ID})$, $R' = e(S, g_2^x \cdot P_{\mathsf{pub}}) \cdot g^{-h}$. Output 1 if $h = \mathsf{H}_2(m \parallel R')$, and 0 otherwise.

A.2 Twisted ElGamal Public Key Encryption

The Twisted ElGamal [10] is a zero-knowledge friendly encryption scheme based on the DDH assumption. It consists of the following four PPT algorithms:

- $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$: Generate a cyclic group $\mathbb{G}$ of prime order q with generators $g, h \in \mathbb{G}$ such that $\log_g h$ is unknown. Output $\mathsf{pp} = (\mathbb{G}, q, g, h)$.
- $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$: Sample $\mathsf{sk} \leftarrow\$ \mathbb{Z}_q^*$ and set $\mathsf{pk} = g^{\mathsf{sk}}$.
- $c \leftarrow \mathsf{Encrypt}(\mathsf{pk}, m)$: Sample $r \leftarrow\$ \mathbb{Z}_q^*$. Output $c = (c_0, c_1) = (\mathsf{pk}^r, g^r h^m)$.
- $m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, c)$: Parse $c = (c_0, c_1)$ and compute $h^m = c_1 / c_0^{\mathsf{sk}^{-1}}$. Recover m from h^m.

Decryption requires solving a discrete logarithm to the base h, and is therefore efficient only when the message space is small (e.g., $m \in [0, 2^{32}]$ or $m \in \Phi$ for a predefined set Φ).

A.3 Signatures of Knowledge

Let $\mathcal{R}$ be a polynomial time recognizable relation and $\mathcal{L}_{\mathcal{R}} := \{s \mid \exists w, \text{ s.t.}(s, w) \in \mathcal{R}\}$ denote the language associated with $\mathcal{R}$. A signature of knowledge scheme SoK for the relation $\mathcal{R}$ typically consists of the following PPT algorithms:

- $\mathsf{Setup}(\lambda) \to \mathsf{pp}$: It takes as input the security parameter λ and outputs the public parameters pp, which implicitly define a relation $\mathcal{R}$.
- $\mathsf{Sign}(s, w, m) \to \sigma$: It takes as input a statement s, a witness w, and a message $m \in \{0,1\}^*$ and outputs a signature of knowledge σ on m.
- $\mathsf{Verify}(s, m, \sigma) \to \{0,1\}$: It takes as input a statement s, a message m, and a signature σ, and outputs 1 if the signature is valid and 0 otherwise.

A signature of knowledge scheme should be simulatable and extractable. Refer to [7] for formal definitions of these properties.

B Missing Proofs

Theorem 4 (Linkability). *Assuming the unforgeability of the* BLMQ-RLRS *scheme and the soundness of the relation $\mathcal{R}'$, the* BLMQ-RLRS *scheme achieves linkability in the random oracle model.*

Proof. Suppose a PPT adversary $\mathcal{A}$ wins SigLink with non-negligible advantage. Since σ_1 and σ_2 are valid, soundness guarantees an extractor $\mathcal{E}$ can recover witnesses (d_{ID_1}, x_1) and (d_{ID_2}, x_2) satisfying $e(d_{\mathsf{ID}_i}, g_2^{x_i} \cdot P_{\mathsf{pub}}) = e(g_1, g_2), i \in \{1, 2\}$. Furthermore, the linking tag is defined as $I = e(d_{\mathsf{ID}}, H_7(\mathsf{event}))$. For the shared event^*, let $U = H_7(\mathsf{event}^*)$. The extracted tags are $I_1 = e(d_{\mathsf{ID}_1}, U)$ and $I_2 = e(d_{\mathsf{ID}_2}, U)$. We consider two cases:

- **Case 1:** $d_{\mathsf{ID}_1} = d_{\mathsf{ID}_2}$. The determinism of the bilinear pairing $e(\cdot, \cdot)$ strictly implies that $I_1 = e(d_{\mathsf{ID}_1}, U) = e(d_{\mathsf{ID}_2}, U) = I_2$. Consequently, the linking algorithm will output 1, which contradicts $\mathcal{A}$'s winning condition.
- **Case 2:** $d_{\mathsf{ID}_1} \neq d_{\mathsf{ID}_2}$. Since $\mathcal{A}$ queried $\mathcal{O}_{\mathsf{KeyExt}}$ for at most one identity (let its key be d_{corr}), at least one extracted key $d_{\mathsf{ID}^*} \in \{d_{\mathsf{ID}_1}, d_{\mathsf{ID}_2}\}$ must satisfy $d_{\mathsf{ID}^*} \neq d_{corr}$. This implies $\mathcal{A}$ successfully derived a valid private key for an uncorrupted identity, which contradicts the unforgeability of the scheme.

Therefore, no PPT adversary can win the SigLink game with a non-negligible advantage, concluding that the proposed scheme achieves linkability. □

Theorem 5 (Non-slanderability). *Assuming the unforgeability and linkability of the* BLMQ-RLRS*, it achieves non-slanderability in the random oracle model.*

Proof. Suppose there exists a PPT adversary $\mathcal{A}$ that wins SigSland with a non-negligible advantage. By soundness, $\mathcal{E}$ could extract a valid private key d' from σ'. The linking tag collision $I' = I^*$ implies $e(d', U) = e(d_{\mathsf{ID}^*}, U)$. Due to pairing non-degeneracy and $U \neq 1$, we have $d' = d_{\mathsf{ID}^*}$. Thus, $\mathcal{A}$ implicitly derives a valid private key for the uncorrupted identity ID^*. This directly breaks the unforgeability of the underlying scheme, which occurs with negligible probability. □

Theorem 6 (Revocability). *Assuming the unforgeability of the* BLMQ-RLRS *and the soundness of the relation $\mathcal{R}'$, the* BLMQ-RLRS *scheme achieves revocability in the random oracle model.*

Proof. Suppose a PPT adversary $\mathcal{A}$ wins SigRevoke. By soundness, the extractor $\mathcal{E}$ recovers a witness $(x_\pi, d_{\mathsf{ID}_\pi}, \boldsymbol{b_L}, \boldsymbol{b_R}, r_1, r_2)$ from σ^*. During revocation, the RA uses $\mathsf{sk}_R = d_R$ to compute $M = A_1^* \cdot (A_0^*)^{-d_R^{-1}} = g_1^{x_\pi}$ and revealing ID_π. We analyze two exhaustive cases:

- **Case 1:** $\mathsf{ID}_\pi \notin L^*$. The extracted one-hot vector $\boldsymbol{b_L}$ binds A_1^* to a legitimate member of L^*. Outputting this signature reduces directly to breaking the soundness of the relation $\mathcal{R}'$, bounded by a negligible advantage $\epsilon_{\mathsf{sok_sound}}$. Specifically, when $\mathcal{A}$ corrupts all members in the ring (i.e. $L^* \subseteq \mathcal{Q}_{\mathsf{KeyExt}}$), it can only attempt to win by forging a valid signature of knowledge.

– **Case 2:** $\mathsf{ID}_\pi \in L^*$ but $\mathsf{ID}_\pi \notin \mathcal{Q}_{\mathsf{KeyExt}}$. Here, $\mathcal{A}$ generates a valid signature traced to an uncorrupted identity. This scenario encompasses the extreme case where $L^* \cap \mathcal{Q}_{\mathsf{KeyExt}} = \emptyset$, and it directly breaks the scheme's existential unforgeability, bounded by a negligible advantage $\epsilon_{\mathsf{euf\text{-}cmia}}$.

Consequently, $\mathcal{A}$'s overall advantage is bounded by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{sigrevoke}}(\lambda) \leq \epsilon_{\mathsf{sok_sound}} + \epsilon_{\mathsf{euf\text{-}cmia}}$, which is negligible. □

Theorem 7 (Revocation Soundness). *If the Chaum-Pedersen protocol satisfies soundness and the underlying signature of knowledge satisfies soundness, then our scheme achieves revocation soundness against malicious RA.*

Proof. Suppose a PPT malicious RA $\mathcal{A}$ wins RevSound by outputting a valid proof π^*_{dec} falsely implicating ID^*. Let x_π be the identity hash of the actual signer. By definition, the ciphertext components are $A_0 = \mathsf{pk}_R^{r_1} = h^{d_R r_1}$ and $A_1 = g_1^{x_\pi} h^{r_1}$. We consider two cases for x_π:

– **Case 1:** $x_\pi \neq \mathsf{H}_1(\mathsf{ID}^*)$**.** Then $B^* = A_1 / g_1^{\mathsf{H}_1(\mathsf{ID}^*)}$ simplifies to $g_1^{x_\pi - \mathsf{H}_1(\mathsf{ID}^*)} h^{r_1}$. Since $x_\pi \neq \mathsf{H}_1(\mathsf{ID}^*)$, $(B^*)^{d_R} \neq h^{d_R r_1} = A_0$. Thus, $(h, \mathsf{pk}_R, B^*, A_0)$ is not a valid DDH tuple. Generating a verifying proof π^*_{dec} for an invalid tuple breaks the soundness of the Chaum-Pedersen protocol (bounded by $\epsilon_{\mathsf{cp_sound}}$).
– **Case 2:** $x_\pi = \mathsf{H}_1(\mathsf{ID}^*)$**.** The signature σ^* is genuinely bound to the framed user ID^*. Since $\mathcal{A}$ never queried d_{ID^*}, it means that $\mathcal{A}$ constructed a valid signature of knowledge without the witness. This breaks the soundness of the relation $\mathcal{R}'$ (bounded by $\epsilon_{\mathsf{sok_sound}}$).

Consequently, $\mathcal{A}$'s overall advantage is bounded by $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{revsound}}(\lambda) \leq \epsilon_{\mathsf{cp_sound}} + \epsilon_{\mathsf{sok_sound}}$, which is negligible. □

References

1. Barreto, P.S., Libert, B., McCullagh, N., Quisquater, J.J.: Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: International conference on the theory and application of cryptology and information security. pp. 515–532. Springer (2005)
2. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. Journal of Cryptology **22**(1), 114–138 (2009)
3. Beullens, W., Katsumata, S., Pintore, F.C.: Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 464–492 (2022)
4. Bootle, J., Cerulli, A., Chaidos, P., Ghadafi, E., Groth, J., Petit, C.: Short accountable ring signatures based on ddh. In: European Symposium on Research in Computer Security. pp. 243–265. Springer (2015)
5. Brakerski, Z., Kalai, Y.T.: A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Cryptology ePrint Archive (2010)
6. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: Short proofs for confidential transactions and more. In: 2018 IEEE symposium on security and privacy (SP). pp. 315–334. IEEE (2018)

7. Chase, M., Lysyanskaya, A.: On signatures of knowledge. In: Annual International Cryptology Conference. pp. 78–96. Springer (2006)
8. Chaum, D., Pedersen, T.P.: Wallet databases with observers. In: Annual international cryptology conference. pp. 89–105. Springer (1992)
9. Chaum, D., Van Heyst, E.: Group signatures. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 257–265. Springer (1991)
10. Chen, Y., Ma, X., Tang, C., Au, M.H.: PGC: Decentralized confidential payment system with auditability. In: European Symposium on Research in Computer Security. pp. 591–610. Springer (2020)
11. Fujisaki, E., Suzuki, K.: Traceable ring signature. In: International Workshop on Public Key Cryptography. pp. 181–200. Springer (2007)
12. Groth, J., Kohlweiss, M.: One-out-of-many proofs: Or how to leak a secret and spend a coin. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 253–280. Springer (2015)
13. Hui, X., Chau, S.C.K.: Llring: logarithmic linkable ring signatures with transparent setup. In: European Symposium on Research in Computer Security. pp. 299–319. Springer (2024)
14. Kabaleeshwaran, R., Kishan, B.K.: Efficient revocable linkable ring signatures. In: International Conference on Cryptology in India. pp. 305–325. Springer (2024)
15. Liu, D.Y., Liu, J.K., Mu, Y., Susilo, W., Wong, D.S.: Revocable ring signature. Journal of Computer Science and Technology **22**(6), 785–794 (2007)
16. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for ad hoc groups. In: Australasian conference on information security and privacy. pp. 325–335. Springer (2004)
17. Nassurdine, M., Zhang, H., Zhang, F.: Identity based linkable ring signature with logarithmic size. In: International Conference on Information Security and Cryptology. pp. 42–60. Springer (2021)
18. Nguyen, L.: Accumulators from bilinear pairings and applications to id-based ring signatures and group membership revocation. Topics in Cryptology-CT-RSA 2005 pp. 275–292 (2005)
19. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: International conference on the theory and application of cryptology and information security. pp. 552–565. Springer (2001)
20. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Workshop on the theory and application of cryptographic techniques. pp. 47–53. Springer (1984)
21. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. cryptology eprint archive (2004)
22. Yuen, T.H., Sun, S.f., Liu, J.K., Au, M.H., Esgin, M.F., Zhang, Q., Gu, D.: Ringct 3.0 for blockchain confidential transaction: Shorter size and stronger security. In: International Conference on Financial Cryptography and Data Security. pp. 464–483. Springer (2020)
23. Zhang, F., Kim, K.: Id-based blind signature and ring signature from pairings. In: International conference on the theory and application of cryptology and information security. pp. 533–547. Springer (2002)
24. Zhang, X., Liu, J.K., Steinfeld, R., Kuchta, V., Yu, J.: Revocable and linkable ring signature. In: International Conference on Information Security and Cryptology. pp. 3–27. Springer (2019)
25. Zhaolu, T., Wan, Z., Wang, H.: Division of regulatory power: Collaborative regulation for privacy-preserving blockchains. IEEE Transactions on Information Forensics and Security **19**, 2533–2548 (2023)