2006

Constant-size ID-based linkable and revocable-iff-linked ring signature

Man Ho Allen Au
University of Wollongong, aau@uow.edu.au

Joseph K. Liu
University of Bristol

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Tsz Hon Yuen
The Chinese University of Hong Kong, thy738@uow.edu.au

Constant-size ID-based linkable and revocable-iff-linked ring signature

Abstract

In this paper, we propose a new notion called *Revocable-iff-Linked Ring Signature* (R-iff-L Ring Signature). In R-iff-L ring signatures, a signer can sign on behalf of the whole group, just like ordinary ring signatures. However, if he signs twice or more, he can be linked and his identity can be revoked by everyone. We formally define a new security model for the new notion in identity-based (ID-based) setting and propose a constant-size ID-based construction, that is, the size of the signature is *independent* of the size of the group. In addition, we enhance the security model of ID-based linkable ring signature scheme and provide an implementation with constant size setting. Both schemes are provably secure in our new model.

Disciplines

Physical Sciences and Mathematics

Publication Details

Au, M., Liu, J., Susilo, W. & Yuen, T. (2006). Constant-size ID-based linkable and revocable-iff-linked ring signature. In R. Barua & T. Lange (Eds.), International Conference on Cryptology in India (pp. 364-378). Berlin, Germany: Springer-Verlag.

Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature

Man Ho Au[1], Joseph K. Liu[2], Willy Susilo[1], and T. H. Yuen[3]

[1] Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong
Wollongong 2522, Australia
{aau,wsusilo}@uow.edu.au

[2] Cryptography and Security Department
Institute for Infocomm Research
Singapore
ksliu@i2r.a-star.edu.sg

[3] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
thyuen4@ie.cuhk.edu.hk

Abstract. In this paper, we propose a new notion called *Revocable-iff-Linked Ring Signature* (R-iff-L Ring Signature). In R-iff-L ring signatures, a signer can sign on behalf of the whole group, just like ordinary ring signatures. However, if he signs twice or more, he can be linked and his identity can be revoked by everyone. We formally define a new security model for the new notion in identity-based (ID-based) setting and propose a constant-size ID-based construction, that is, the size of the signature is *independent* of the size of the group.

In addition, we point out some possible attacks on linkable ring signature with ID-based setting *only* and enhance the security model to cover these attacks. We also propose an ID-based event-oriented linkable ring signature scheme with constant size implementation.

Both schemes are provably secure in our new model.

Keywords: Anonymity, Linkable, Revocable, Ring Signature

1 Introduction

Group-oriented cryptography refers to cryptographic systems in which a group of users are involved. In schemes where participation of one or a proper subset of members is required to complete a process, anonymity refers to whether participants are distinguishable from non-participants. According to [2], anonymity for group-oriented cryptography can be divided into 7 different levels, namely, *Full Anonymity*, *Linkable Anonymity*, *Revocable-iff-Linked Anonymity*, *Revocable Anonymity*, *Linkable and Revocable Anonymity*, *Revocable-iff-Linked and*

Revocable Anonymity and *No Anonymity*. Examples of group-oriented cryptographic schemes with different levels of anonymity are shown in the following table while interested readers can refer to [2] for a more detailed discussion.

Anonymity Level	Examples	Size	Event-Oriented	Ad-hoc
Full	Ring Sign[14]	O(n)	N/A	✓
	Anon Ident[9, 12]	O(1)	N/A	✓
Linkable	Linkable Ring[11]	O(n)	×	✓
	Eo-Linkable Ring[19]	O(n)	✓	✓
Revocable-iff-Linked				
2-times	E-Cash[6, 1],TbL[20]	O(1)	×	×
	this paper	O(1)	✓	✓
k-times	Compact E-Cash[7]	O(1)	×	×
	k-TAA[16]	O(k)	✓	×
	dynamic k-TAA[13]	O(k)	✓	✓
	constant-size K-TAA[17]	O(1)	✓	×
	k-Times Group Signature [2]	O(1)	✓	×
Full+OA	Group Signatures	O(1)	×	×
Link+OA	Fair E-Cash[8, 18]	O(1)	×	×

Fig. 1. Examples of group-oriented cryptographic schemes with different levels of anonymity.

Identity-based Cryptography. In 1984, Shamir [15] introduced the notion of Identity-based (ID-based) cryptography to simplify certificate management. The unique feature of ID-based cryptography is that a user's public key can be any arbitrary string. Since then, many other ID-based signature schemes have been proposed, despite the fact that the first practical ID-based encryption appeared only until 2001 [5]. In 2004, Bellare et al. [3] developed a framework to analyze the security of ID-based signature schemes and they proved the security (or insecurity) of 14 schemes found in the literature. As in the case of standard signature, there are also blind signature [22], proxy signature [21], proxy blind signature [10], ring signature [22] in the paradigm of ID-based cryptography.

In the case of ID-based ring signature, we have to take extra care for the design of schemes. While some of the existing schemes provide anonymity *unconditionally*, others are computational only. The Private Key Generator (PKG) itself may have extra advantage in breaking the anonymity since it is in possession of all the private keys. This problem does not sound serious in normal ID-based ring signature scheme because almost all existing schemes is unconditionally anonymous. However, in the case of linkable ring signatures, it is still an open problem to construct one with unconditional anonymity. Within the constraint of computational anonymity, it is a great challenge of providing privacy in an ID-based setting (to the PKG). We require special attention in the design of the scheme.

1.1 Contribution

In this paper, we propose a new notion called *Revocable-iff-Linked Ring Signature* which belongs to the Revocable-iff-Linked Anonymity category. In addition, we have the following contributions:

- We formally define a new security model for this notion, in an ID-based setting.
- We provide a constant size concrete implementation. When compared with the scheme in [2], we do not require any setup or group manager. The formation is spontaneous and is suitable for ad-hoc environment, which is a nice inherited property of ring signature.
- We propose a constant size ID-based ring signature scheme which is secure in the enhanced security model.

Organization. The rest of the paper is organized as follow. The enhanced security models of ID-based Linkable Ring Signature scheme and ID-based Revocable-iff-Linked Ring Signature scheme are given in Section 3. Our concrete implementations are presented in Section 4. We conclude the paper in Section 5.

2 Preliminaries

2.1 Notations

Let $\hat{e}$ be a bilinear map such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

- $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclic multiplicative groups of prime order p.
- each element of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ has unique binary representation.
- g_0, h_0 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.
- $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ is a computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(h_0) = g_0$.
- (Bilinear) $\forall x \in \mathbb{G}_1$, $y \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$.
- (Non-degenerate)$\hat{e}(g_0, h_0) \neq 1$.

$\mathbb{G}_1$ and $\mathbb{G}_2$ can be same or different groups. We say that two groups $(\mathbb{G}_1, \mathbb{G}_2)$ are a bilinear group pair if the group action in $\mathbb{G}_1$, $\mathbb{G}_2$, the isomorphism ψ and the bilinear mapping $\hat{e}$ are all efficiently computable.

2.2 Mathematical Assumptions

Definition 1 (Discrete Logarithm). *The Discrete Logarithm (DL) problem in $\mathbb{G}$ is defined as follows: On input a tuple $(Y, g) \in \mathbb{G}^2$ such that $|\mathbb{G}| = p$ for some prime p, output $a \in \mathbb{Z}_p$ such that $Y = g^a$. We say that the (t, ϵ)-DDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the DL problem in $\mathbb{G}$.*

Definition 2 (Decisional Diffie-Hellman). *The Decisional Diffie-Hellman (DDH) problem in $\mathbb{G}$ is defined as follows: On input a quadruple $(g, h, g^a, T) \in \mathbb{G}^4$ such that $|\mathbb{G}| = p$ for some prime p, output 1 if $T = h^a$ and 0 otherwise. We say that the (t, ϵ)-DDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ over random guessing in solving the DDH problem in $\mathbb{G}$.*

Definition 3 (q-Strong Diffie-Hellman). *The q-Strong Diffie-Hellman (q-SDH) problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follow: On input a $(q+2)$-tuple $(g_0, h_0, h_0^x, h_0^{x^2}, \cdots, h_0^{x^q}) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, output a pair (A, c) such that $A^{(x+c)} = g_0$ where $c \in \mathbb{Z}_p^*$. We say that the (q, t, ϵ)-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no t-time algorithm has advantage at least ϵ in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.*

The q-SDH assumption is shown to be true in the generic group model [4].

3 Security Model

3.1 Definition

The security definition of ID-Based Linkable Ring Signature and ID-Based Revocable-iff-Linked Ring Signature are very similar. Therefore we describe the security notions of them together, and their differences are specified at appropriate places.

An ID-Based Linkable (or Revocable-iff-Linked) Ring Signature scheme is a tuple of probabilistic polynomial-time (PPT) algorithms below:

- **Setup**. On input an unary string 1^λ where λ is a security parameter, the algorithm outputs a master secret key s and a list of system parameters param that includes λ and the descriptions of a user secret key space $\mathcal{D}$, a message space $\mathcal{M}$ as well as a signature space Ψ.
- **Extract**. On input a list param of system parameters, an identity $ID_i \in \{0,1\}^*$ for a user and the master secret key s, the algorithm outputs the user's secret key $d_i \in \mathcal{D}$. When we say identity ID_i corresponds to user secret key d_i or vice versa, we mean the pair (ID_i, d_i) is an input-output pair of **Extract** with respect to param and s. Usually this algorithm is executed by a trusted party called Private Key Generator (PKG).
- **Sign**. On input a list param of system parameters, a group size n of length polynomial in λ, a set $\{ID_i \in \{0,1\}^* | i \in [1,n]\}$ of n user identities, a message $m \in \mathcal{M}$, and a secret key $\{d_j \in \mathcal{D} | j \in [1,n]\}$, the algorithm outputs an ID-based linkable (or revocable-iff-linked) ring signature $\sigma \in \Psi$.
- **Verify**. On input a list param of system parameters, a group size n of length polynomial in λ, a set $\{ID_i \in \{0,1\}^* | i \in [1,n]\}$ of n user identities, a message $m \in \mathcal{M}$, a signature $\sigma \in \Psi$, it outputs either valid or $\mathsf{invalid}$.
- **Link**. On input two signatures $\sigma_1, \sigma_2 \in \Psi$, it outputs either link or unlink.
- **Revoke**. (For ID-based revocable-iff-linked ring signature only.) On input two signatures $\sigma_1, \sigma_2 \in \Psi$ such that $\mathsf{link} \leftarrow \mathbf{Link}(\sigma_1, \sigma_2)$, it outputs ID.

Correctness. An ID-Based Linkable Ring Signature scheme should satisfy:

- *Verification Correctness* – Signatures signed by honest signers are verified to be invalid with negligible probability.
- *Linking Correctness* – If two signatures are linked, they must be generated from the same secret key of the same signer.

For ID-Based Revocable-iff-Linked Ring Signature, the *Revoking Correctness* requires that the output of **Revoke** of two linked signatures must be the actual signer.

3.2 Security Requirement of ID-based Linkable Ring Signature

A secure ID-Based Linkable Ring Signature scheme should possess *unforgeability*, *anonymity*, *linkability* and *non-slanderability* which will be defined below.

Unforgeability. An adversary should not be able to forge any signature just from the identities of the group members. We specify a security model which mainly captures the following two attacks:

1. Adaptive chosen message attack
2. Adaptive chosen identity attack

Adaptive chosen message attack allows an adversary to obtain message-signature pairs on demand during the forging attack. Adaptive chosen identity attack allows the adversary to forge a signature with respect to a group chosen by the adversary. To support adaptive chosen message attack, we provide the adversary the following oracle queries.

- **Extraction oracle ($\mathcal{EO}$):** On input ID_i, $d_i \leftarrow$ **Extract**$(\mathsf{param}, ID_i, s)$ is returned . The oracle is stateful, meaning that if $ID_i = ID_j$, then $d_i = d_j$.
- **Signing oracle ($\mathcal{SO}$):** $\mathcal{A}$ chooses a group of n identities $\{ID_i\}_{i\in[1,n]}$, a signer identity ID_j among them and a message m, the oracle outputs a valid ID-based linkable (or revocable-iff-linked) ring signature denoted by $\sigma \leftarrow$ **Sign**$(\mathsf{param}, n, \{ID_i | i \in [1, n]\}, m, d_j)$. The signing oracle may query the extraction oracle during its operation.
- **Hash oracle ($\mathcal{H}$):** $\mathcal{A}$ can ask for the values of the hash functions for any input.

We have the following unforgeability game:

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

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

1. **Verify**$(\mathsf{param}, |L^*|, L^*, m^*, \sigma^*) = \mathsf{valid}$;
2. (L^*, m^*) and σ^* should not be in the set of oracle queries and replies between $\mathcal{A}$ and $\mathcal{SO}$; and
3. $\mathcal{A}$ did not query $\mathcal{EO}$ on any identity $ID \in L^*$.

The advantage of $\mathcal{A}$ is defined as the probability that $\mathcal{A}$ wins.

Definition 4 (Unforgeability). *A scheme is unforgeable if no PPT adversary has non-negligible advantage in winning the above game.*

L-Anonymity. An adversary should not be able to tell the identity of the signer with a probability larger than $1/n$, where n is the cardinality of the ring. A crucial difference between Anonymity for ring signatures and L-Anonymity for linkable ring signatures is that in the latter, the adversary cannot query signatures of a user who appears in the challenge phase. The rationale is that if the adversary obtains signature of user i, it can tell if the challenge signature is generated by this user due to the linking property.

Different from a non-ID-based linkable ring signature scheme, the PKG who knows the master secret key (thus it knows the secret key of every user), may gain advantage on the anonymity of a signature. In order to capture this potential attack, we enhance our model in a way that the adversary is also given the master secret key.

In order to capture the potential attack, we further define the following oracle:

- **Reversed Extraction oracle** ($\mathcal{REO}$)**:** The only difference between $\mathcal{REO}$ and the traditional $\mathcal{EO}$ is that, it is simulated by the adversary instead of the simulator. The initial request can be made by the adversary if the extracted protocol is an interactive one. In this case, the simulator acts as an honest user to provide interactions and the oracle records the necessary transcript of the interaction. Note that this maybe different from the final output of the interaction protocol due to some secret information which is only known to the honest user.

We have the following anonymity game:

1. A simulator $\mathcal{S}$ takes a sufficiently large security parameter λ and runs **Setup** to generate the public parameters param and master secret key s. The adversary $\mathcal{A}$ is given param and s.
2. $\mathcal{A}$ can make a polynomial number of oracle queries to $\mathcal{REO}$, $\mathcal{SO}$ and $\mathcal{H}$ adaptively.
3. In the challenge phase, $\mathcal{A}$ picks two identities ID_1^*, ID_2^*, which are not queried to the $\mathcal{SO}$ as a signer. $\mathcal{A}$ also picks a message m^* and a set of n identities L^*. Then $\mathcal{A}$ receives a challenge signature $\sigma^* = \mathbf{Sign}(\mathsf{param}, n+2, L^* \cup \{ID_1^*, ID_2^*\}, m^*, d_{ID_b^*})$, where $b \in \{0, 1\}$.
4. $\mathcal{A}$ can queries oracles $\mathcal{REO}$, $\mathcal{SO}$ and $\mathcal{H}$ adaptively, where ID_1^*, ID_2^* are not queried to the $\mathcal{SO}$ as a signer.
5. Finally $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$.

$\mathcal{A}$ wins the above game if $b = b'$. The advantage of $\mathcal{A}$ is defined as the probability that $\mathcal{A}$ wins minus 1/2.

Definition 5 (Anonymity). *A scheme is anonymous if no PPT adversary has non-negligible advantage in winning the above game.*

Note 1: Although the adversary has the master secret key and it can generate an additional secret key for ID_1^* or ID_2^*, this secret key is different from the one owned by ID_1^* or ID_2^* (generated by $\mathcal{REO}$). According to our definition of *Linking Correctness*, those signatures generated by these two secret keys cannot be linked, although they are corresponding to the same identity.

Linkability. An adversary should not be able to form two signatures with the same secret key without being linked by the **Link** protocol.

We have the following linkability game:

1. A simulator $\mathcal{S}$ takes a sufficiently large security parameter λ and runs **Setup** to generate the public parameters param and master secret key s. The adversary $\mathcal{A}$ is given param.
2. $\mathcal{A}$ can make a polynomial number of oracle queries to $\mathcal{EO}$, $\mathcal{SO}$ and $\mathcal{H}$ adaptively.
3. $\mathcal{A}$ outputs signatures σ_i^* for messages m_i^* and rings L_i^* for $i \in \{0, 1\}$.

Let C be the set of identities queried to $\mathcal{EO}$. $\mathcal{A}$ wins the above game if:

- σ_0 and σ_1 are not outputs from $\mathcal{SO}$.
- $\mathbf{Verify}(\mathsf{param}, |L_i^*|, L_i^*, m_i^*, \sigma_i^*) = \mathsf{valid}$ for $i \in \{0, 1\}$;
- $\mathbf{Link}(\sigma_0^*, \sigma_1^*) = \mathsf{Unlink}$; and
- $|(L_0^* \cup L_1^*) \cap C| \leq 1$.

The advantage of $\mathcal{A}$ is defined as the probability that $\mathcal{A}$ wins.

Definition 6 (Linkability). *A scheme is linkable if no PPT adversary has non-negligible advantage in winning the above game.*

Non-slanderability. Informally speaking, non-slanderability ensure that no adversary, can frame an honest user for signing a signature. That is, an adversary cannot produce a valid signature that is linked to a signature generated by a user. In addition to the above oracles, we define one more:

- **Challenged Signing oracle** ($\mathcal{CSO}$)**:** The only difference between $\mathcal{CSO}$ and the traditional $\mathcal{SO}$ is that, it requires the simulator to use the secret key queried from the $\mathcal{REO}$ and execute **Sign** algorithm specified in the scheme to generate the signature. $\mathcal{REO}$ should be queried before if necessary.

Formally it is defined as follow:

1. A simulator $\mathcal{S}$ takes a sufficiently large security parameter λ and runs **Setup** to generate param and master secret key s. $\mathcal{S}$ sends param and s to the adversary $\mathcal{A}$.

2. $\mathcal{A}$ makes a polynomial number of oracle queries to $\mathcal{REO}$ and $\mathcal{H}$ in an adaptive manner.
3. $\mathcal{A}$ submits a polynomial number of oracle queries to $\mathcal{CSO}$ adaptively for generating challenged signatures.
4. $\mathcal{A}$ outputs a signature σ^* for message m^* and ring L^*.

$\mathcal{A}$ wins the game if

- **Verify**$(\mathsf{param}, |L^*|, L^*, m^*, \sigma^*)$ returns valid.
- σ^* is not an output of any $\mathcal{CSO}$ query.
- **Link**$(\sigma^*, \hat{\sigma}) = \mathsf{Link}$ where $\hat{\sigma}$ is any signature outputted from $\mathcal{CSO}$.

Definition 7 (Non-slanderability). *A scheme is non-slanderability if no PPT adversary has non-negligible advantage in winning the above game.*

Note 2: Although the adversary may initialize the query of $\mathcal{REO}$, it cannot get the user secret key since it does not know some secret information which is only known to the honest user (that is, the simulator in this game). Thus it cannot generate a signature by that particular secret key which is linked together with some signatures outputted by $\mathcal{CSO}$. In addition, the remark of Note 1 also applies here.

Theorem 1. *For an ID-based linkable ring signature scheme, if it is linkable and non-slanderable, it implies that it is unforgeable.*

Proof. (sketch) We assume that the scheme is linkable and non-slanderable. Suppose there exists an adversary $\mathcal{A}$ who can forge the signature with non-negligible probability. $\mathcal{A}$ plays the game in Linkability. It submits one query to $\mathcal{EO}$ and produces a signature using this secret key. It forges another signature with another identity as the actual signer. Obviously these two signatures are unlink. That is, it breaks linkability, contradicts our assumption. □

3.3 Security Requirement of ID-based Revocable-iff-Linkable Ring Signature

The definitions of unforgeability and anonymity are the same as ID-based Linkable Ring Signature defined in Section 3.2. We skip here.

Revoke-iff-Linkability. An adversary should not be able to form two signatures with the same secret key without being linked by the **Link** protocol or pointed to a user outside the rings.

We have the following linkability game:

1. A simulator $\mathcal{S}$ takes a sufficiently large security parameter λ and runs **Setup** to generate the public parameters param and master secret key s. The adversary $\mathcal{A}$ is given param.
2. $\mathcal{A}$ can make a polynomial number of oracle queries to $\mathcal{EO}$, $\mathcal{SO}$ and $\mathcal{H}$ adaptively.

3. $\mathcal{A}$ outputs signatures σ_i^* for messages m_i^* and rings L_i^* for $i \in \{0,1\}$.

Let C be the set of identities queried to $\mathcal{EO}$. $\mathcal{A}$ wins the above game if it fulfils either condition:

1. – σ_0 and σ_1 are not outputs from $\mathcal{SO}$.
   – **Verify**$(\mathsf{param}, |L_i^*|, L_i^*, m_i^*, \sigma_i^*) = \mathsf{valid}$ for $i \in \{0,1\}$;
   – **Link**$(\sigma_0^*, \sigma_1^*) = \mathsf{Unlink}$; and
   – $|(L_0^* \cup L_1^*) \cap C| \leq 1$.

   OR
2. – σ_0 and σ_1 are not outputs from $\mathcal{SO}$.
   – **Verify**$(\mathsf{param}, |L_i^*|, L_i^*, m_i^*, \sigma_i^*) = \mathsf{valid}$ for $i \in \{0,1\}$;
   – **Link**$(\sigma_0^*, \sigma_1^*) = \mathsf{Link}$; and
   – **Revoke**$(\sigma_0^*, \sigma_1^*) = ID'$ where $ID' \notin \{L_0^* \cup L_1^*\}$ or ID' has not been inputted to $\mathcal{EO}$.

The advantage of $\mathcal{A}$ is defined as the probability that $\mathcal{A}$ wins.

Definition 8 (Revoke-iff-Linkability). *A scheme is revocable-iff-linked if no PPT adversary has non-negligible advantage in winning the above game.*

Non-slanderability. The non-slanderability includes the one defined above in Section 3.2 (Def. 7) and the definition of Revoke-iff-linkability (Def. 8).

Definition 9 (Non-slanderability). *A scheme is non-slanderable if no PPT adversary has non-negligible advantage in winning the games defined in Def. 7 and Def. 8.*

4 Our Proposed Schemes

4.1 Construction

System Setup:

- **Init (Common parameter):** Let λ be the security parameter. Let $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group pair with computable isomorphism ψ such that $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p of λ bits. Let $H : \{0,1\}^* \to \mathbb{Z}_p$, be a cryptographic hash function. Also assume $\mathbb{G}_p$ be a group of order p where DDH is intractable. Let g_0, g_1, g_2 be generators of $\mathbb{G}_1$, h_0, h_1, h_2 be generators of group $\mathbb{G}_2$ such that $\psi(h_i) = g_i$ for $i = 0, 1, 2$ and u_0, u_1, u_2 be generators of $\mathbb{G}_p$ such that relative discrete logarithm of the generators are unknown. This can be done by setting the generators to be output of a hash function of some publicly known seed.
- **Init (Accumulator):** Choose a generator h of $\mathbb{G}_2$. Randomly select $q \in_R \mathbb{Z}_p^*$ and compute $q_i = h^{(q^i)}$ for $i = 1 \cdots t_{max}$, where t_{max} is the maximum number of accumulation.

PKG Setup: The PKG randomly selects $\gamma \in_R \mathbb{Z}_p^*$ and compute $w = {h_0}^{\gamma}$. The master secret is γ while the public parameters are $(H, \psi, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_p, p, g_0, g_1, g_2, h_0, h_1, h_2, u_0, u_1, u_2, h, q_1, \ldots, q_{t_{max}}, w)$.

Extract: User with identity ID_u obtain the corresponding secret key from PKG through the following interactive protocol.

1. User with identity ID_u randomly selects $s', r_s \in_R \mathbb{Z}_p^*$ and sends $C' = g_1^{s'} g_2^{r_s}$, along with the proof $\mathit{\Pi}_0 = SPK\{(s', r_s) : C' = g_1^{s'} g_2^{r_s}\}$ to PKG.
2. PKG verifies that $\mathit{\Pi}_0$ is valid. If it is valid, it randomly selects $s'' \in_R \mathbb{Z}_p^*$ and computes
$$C = C' g_1^{s''} \qquad e = H(ID_u) \qquad A = (g_0 C)^{\frac{1}{e+\gamma}}$$
and sends (A, e, s'') to the user.
3. User computes $s = s' + s''$ and checks if $e(A, w h_0^e) = e(g_0 g_1^s g_2^{r_s}, h_0)$. It then stores (A, e, s, r_s).

Sign(Link Version): For signing a message M, compute

$$v = h^{\prod_{k=1}^{k=|\{ID\}|}(q+H(ID_k))} \qquad v_w = h^{\prod_{k=1,k\neq u}^{k=|\{ID\}|}(H(ID_k)+q)} \qquad S = {u_0}^s$$
$$SPK\{(A, e, s, r_s, v_w) : A^{e+\gamma} = g_0 g_1^s g_2^{r_s} \ \wedge \ v_w^{e+q} = v \ \wedge \ S = {u_0}^s\}(M)$$

This can be efficiently constructed as a discrete-log relation SPK, by randomly generating some variables $r_1, r_2, r_e \in_R \mathbb{Z}_p^*$ and computing

$$A_1 = {g_1}^e {g_2}^{r_e}, \quad A_2 = A {g_2}^{r_1}, \quad A_3 = v_w {g_2}^{r_2},$$
$$\alpha_1 = r_1 e, \quad \alpha_2 = r_2 e, \quad \alpha_3 = r_1 r_e, \quad \alpha_4 = r_2 r_e,$$

and producing the following non-interactive zero-knowledge proof-of-knowledge:

$$\begin{aligned}\pi_1 := SPK\{(r_1, r_2\ , r_e, \alpha_1, \alpha_2, \alpha_3, \alpha_4, e, s, r_s) : \\ A_1 = g_1^e g_2^{r_e} \ \wedge \ A_1^{r_1} = g_1^{\alpha_1} g_2^{\alpha_3} \ \wedge \ A_1^{r_2} = g_1^{\alpha_2} g_2^{\alpha_4} \ \wedge \ S = u_0^s \ \wedge \\ \frac{e(A_2, w)}{e(g_0, h_0)} = e(g_1, h_0)^s e(g_2, h_0)^{r_s} e(g_2, w)^{r_1} e(g_2, h_0)^{\alpha_1} e(A_2, h_0)^{-e} \\ \frac{e(A_3, q_1)}{e(v, h)} = e(g_2, q_1)^{r_2} e(g_2, h)^{\alpha_2} e(A_3, h)^{-e} \quad \}(M)\end{aligned}$$

The signature on M is parsed as $(S, A_1, A_2, A_3, \pi_1)$. Note that S is the linkability tag. This can be turned into event-oriented version by replacing u_0 with $G(event)$ where G is some suitable hash function. The signature contains S and the transcript of the SPK.

Sign(Revocable-iff-Link Version): Same as above except adding an extra component T. Specifically, create a signature as in the link version $(S, A_1, A_2, A_3, \pi_1)$ on message M. Let $R = H(S||A_1||A_2||A_3||\pi_1||M)$, compute $T = u_0^e u_1^{Rs}$ and make a proof that T is correctly formed.

This can be done via the following non-interactive zero-knowledge proof-of-knowledge:

$$\pi_2 := SPK\{(e, r_e, s) : A_1 = g_1^e g_2^{r_e} \ \wedge \ S = u_0^s \ \wedge \ T = u_0^e (u_1^R)^s\}(M)$$

Parse the signature on M as $(S, T, A_1, A_2, A_3, \pi_1, \pi_2)$.

Verify: In the link version, parse the signature as $(S, A_1, A_2, A_3, \pi_1)$. Verify the SPK π_1.

In the revocable-iff-link version, parse the signature as $(S, T, A_1, A_2, A_3, \pi_1, \pi_2)$. Compute $R = H(S||A_1||A_2||A_3||\pi_1||M)$ and verify the SPK π_1 and π_2.

Link: Two signatures are linked if the share the same link tag S.

Revoke: Given two signatures $(S, T, A_1, A_2, A_3, \pi_1, \pi_2)$ and $(S, T', A'_1, A'_2, A'_3, \pi'_1, \pi'_2)$ on messages M from ring L and M' from ring L' respectively, computes $R = H(S||A_1||A_2||A_3||\pi_1||M)$ and $R' = H(S||A'_1||A'_2||A'_3||\pi'_1||M')$. Compute $U = (\frac{T^{R'}}{T'^{R}})^{(\frac{1}{R'-R})}$. For each identity ID in $L \cap L'$, output ID if and only if $U = u_0^{H(ID)}$.

We present the following theorem regarding the security of our scheme, whose proof can be found in the Appendix.

Theorem 2. *Our scheme Link version (resp. Revocalbe-iff-Link version) possesses unforgeability, anonymity, linkability (resp. revocable-iff-linkability) and non-slanderability if the q-SDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$ *and the DL assumption holds in* $\mathbb{G}_p$ *in the random oracle model.*

5 Conclusion

In this paper, we proposed a new notion called *Revocable-iff-Linked Ring Signature*. We define a new model in an ID-based setting and provide a constant-size concrete implementation. We also propose an ID-based linkable ring signature scheme with constant size space complexity.

References

1. M. H. Au, S. S. M. Chow, and W. Susilo. Short e-cash. In *INDOCRYPT*, pages 332–346, 2005.
2. M. H. Au, W. Susilo, and S. Yiu. Event-oriented k-times revocable-iff-linked group signatures. In *ACISP*, pages 223–234, 2006.

3. M. Bellare, C. Namprempre, and G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In *EUROCRYPT*, pages 268–286, 2004.
4. D. Boneh and X. Boyen. Short Signatures Without Random Oracles. In *EUROCRYPT*, pages 56–73, 2004.
5. D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO*, pages 213–229, 2001.
6. S. Brands. Untraceable off-line cash in wallets with observers (extended abstract). In *CRYPTO*, pages 302–318, 1993.
7. J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact E-Cash. In *EUROCRYPT*, pages 302–321, 2005.
8. S. Canard and J. Traoré. On Fair E-cash Systems Based on Group Signature Schemes. In R. Safavi-Naini and J. Seberry, editors, *ACISP 2003*, pages 237–248, 2003.
9. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad hoc groups. In *EUROCRYPT*, pages 609–626, 2004.
10. Z. Dong, H. Zheng, K. Chen, and W. Kou. ID-Based Proxy Blind Signature. In *AINA (2)*, pages 380–383, 2004.
11. J. K. Liu, V. K. Wei, and D. S. Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups (Extended Abstract). In *ACISP*, pages 325–335, 2004.
12. L. Nguyen. Accumulators from Bilinear Pairings and Applications. In *CT-RSA*, pages 275–292, 2005.
13. L. Nguyen and R. Safavi-Naini. Dynamic k-Times Anonymous Authentication. Cryptology ePrint Archive, Report 2005/168, 2005. http://eprint.iacr.org/.
14. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *ASIACRYPT*, pages 552–565, 2001.
15. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO*, pages 47–53, 1984.
16. I. Teranishi, J. Furukawa, and K. Sako. k-Times Anonymous Authentication (Extended Abstract). In *ASIACRYPT*, pages 308–322, 2004.
17. I. Teranishi and K. Sake. k-times Anonymous Authentication with a Constant Proving Cost. In *PKC*, 2006.
18. M. Trolin. A universally composable scheme for electronic cash. Cryptology ePrint Archive, Report 2005/341, 2005. http://eprint.iacr.org/.
19. P. P. Tsang, V. K. Wei, T. K. Chan, M. H. Au, J. K. Liu, and D. S. Wong. Separable Linkable Threshold Ring Signatures. In *INDOCRYPT*, pages 384–398, 2004.
20. V. K. Wei. Tracing-by-linking group signatures. In *ISC*, pages 149–163, 2005.
21. J. Xu, Z. Zhang, and D. Feng. ID-Based Proxy Signature Using Bilinear Pairings. Cryptology ePrint Archive, Report 2004/206, 2004. http://eprint.iacr.org/.
22. F. Zhang and K. Kim. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings. In *ACISP*, pages 312–323, 2003.

A Security Analysis

The Revocable-iff-Link Version can be regarded as a generalization of the Link Version. Thus we only show the security analysis of the Revocable-iff-Link Version. In rest of this section, we refer "our scheme" as the proposed ID-Based Revocable-iff-Link Ring Signature scheme.

Theorem 3. *Our scheme is anonymous if the DDH assumption in $\mathbb{G}_p$ holds in the random oracle model.*

Proof. (sketch.) By the zero-knowledge property of the SPK in **Sign**, the parameters computed inside the SPK protocol reveal no information about the signer identity. Therefore only the parameters (A_1, A_2, A_3, S, T) may reveal such information.

Note that A_1 is a commitment of $e = H(ID_u)$, where ID_u is the identity of the signer. Due to the hiding property of the commitment scheme, A_1 leaks no information about e. Specifically, for any value of e, there exists a value r_e such that $A_1 = g_1^e g_2^{r_e}$. Likewise, for any values A and v_w, there exists r_1, r_2 such that $A_2 = A g_2^{r_1}$ and $A_3 = v_w g_2^{r_2}$. Thus, (A_1, A_2, A_3) leaks no information to the adversary as well.

Indeed, the only values containing information about the signer is S and T, which are essential since they provide sufficient information for anyone to identify the signer should he sign twice. However, given a single pair of S and T, the identity of the signer is hidden under the DDH assumption in $\mathbb{G}_p$.

Specifically, let $\mathcal{S}$ be a simulator whose input is u_0, u_1, u_0^s, T and its task is to determine if $T \overset{?}{=} u_1^s$. $\mathcal{S}$ employs the zero-knowledge simulator to simulator all the reversed extraction oracle queries. Then at the challenge phase, $\mathcal{S}$ picks $b \in_R \{0, 1\}$. Suppose the challenge identity is ID_b^*. If ID_b^* corresponds to an reverse extraction oracle query with transcript involving values $(C', s'', C, e = H(ID_b^*), A)$, $\mathcal{S}$ simulates the challenge signature as if ID_b^* is having a secret key of (A, e, s, r_s). Note that in the view of the adversary, it is entirely correct as for any value s, there exists value r_s such that $C = C' g_1^{s''} = g_1^s g_2^{r_s}$. $\mathcal{S}$ then sets the value $S = u_0^s$, $T = u_0^e T^R$ and some random values A_1, A_2, A_3, and simulates π_1 and π_2. $\mathcal{S}$ returns $(A_1, A_2, A_3, S, T, \pi_1, \pi_2)$ as the challenge signature. If $\mathcal{A}$ finally outputs $b' = b$, then $\mathcal{S}$ outputs 1 for the DDH problem. Otherwise, $\mathcal{S}$ outputs 0.

Note that if $T = u_1^s$, the challenge signature is a correct signature produced by the secret key (A, e, s, r_s) which belongs to ID_b^*. Otherwise, it contains no information about ID_b^* in the view of the adversary and thus based on the success of $\mathcal{A}$, $\mathcal{S}$ can solve the DDH problem.

Theorem 4. *Our scheme is non-slanderable if the q-SDH assumption in holds in $(\mathbb{G}_1, \mathbb{G}_2)$ and the DL assumption holds in $\mathbb{G}_p$ in the random oracle model.*

According to definition 9, our scheme is non-slanderable if there is no PPT adversary can win the game in definition 7 and definition 8.

Lemma 1. *There is no PPT adversary has non-negligible advantage in winning the game defined in definition 7 if the DL assumption holds in $\mathbb{G}_p$ in the random oracle model.*

Proof. (Sketch.) We first simulate the game in definition 7. Assume an adversary $\mathcal{A}$ exists. We are going to construct another PPT $\mathcal{S}$ that makes use of $\mathcal{A}$ to solve the DL problem. $\mathcal{S}$ is given the tuple (S^*, u^*) and its task is to output s such that $S^* = {u^*}^s$.

$\mathcal{S}$ generates the parameters honestly except u_0, u_1 is set to be $u^*, u^{*\mu}$ for some random value $\mu \in_R \mathbb{Z}_p$. The parameters and master secret key are given to $\mathcal{A}$.

$\mathcal{S}$ simulates all the $\mathcal{REO}$ and $\mathcal{CSO}$ queries using the zero-knowledge simulator. $\mathcal{S}$ randomly picks one of the identity ID_i in an $\mathcal{REO}$ query, and suppose the transcript involving values $(C', s'', C, e = H(ID_i), A)$, $\mathcal{S}$ simulates this user as if it is having a secret key of (A, e, s, r_s), where s is value of discrete logarithm $\mathcal{S}$ wish to compute. The view provided to $\mathcal{A}$ is correct, since for any value of s, there exists a value r_s such that $C = C' g_1^{s''} = g_1^s g_2^{r_s}$. In an $\mathcal{CSO}$ query involving user ID_i, $\mathcal{S}$ sets $S = S^*$, $T = u_0^e S^{*R\mu}$, A_1, A_2, A_3 to be random values and simulates the signature using the zero-knowledge simulator.

Finally, $\mathcal{A}$ returns a valid signature σ^*, which is not the output from $\mathcal{CSO}$, but is linked to one of them. If it is linked to the signature created from ID_i, $\mathcal{S}$ rewinds and extracts the SPK to obtain s. Then $\mathcal{S}$ returns s as the solution of the DL problem.

Lemma 2. *There is no PPT adversary has non-negligible advantage in winning the game defined in definition 8 if the q-SDH assumption in holds in* $(\mathbb{G}_1, \mathbb{G}_2)$ *in the random oracle model.*

Proof. We then simulate the game in definition 8. Assume an adversary $\mathcal{A}$ exists. We construct another PPT $\mathcal{S}$ that makes use of $\mathcal{A}$ to solve the q-SDH problem.

Setup. $\mathcal{S}$ receives a q-SDH tuple $(g_1', g_2', {g_2'}^{x}, \ldots, {g_2'}^{x^q})$. $\mathcal{S}$ randomly picks $e_1, \ldots e_{q-1} \in \mathbb{Z}_p^*$ and computes $f(x) = \prod_{i=1}^{q-1}(x+e_i)$. If $x = -e_i$ for some i, $\mathcal{S}$ solves the q-SDH problem directly.

$\mathcal{S}$ uses the q-SDH tuple to compute:

$$h_0 = {g_2'}^{f(x)}, \qquad w = {g_2'}^{xf(x)}, \qquad g_0 = \psi(h_0).$$

$\mathcal{S}$ picks $e^*, a^*, k^* \in \mathbb{Z}_p^*$ and computes:

$$h_1 = [(w h_0^{e^*})^{k^*} h_0^{-1}]^{1/a^*} = h_0^{\frac{(e^*+x)k^*-1}{a^*}}, \qquad g_1 = \psi(h_1).$$

$\mathcal{S}$ randomly picks $\mu \in \mathbb{Z}_p^*, h \in \mathbb{G}_2$, sets $g_2 = g_0^{\mu}$ and sets q_i accordingly. $\mathcal{S}$ computes:

$$A_i = g_0^{1/x+e_i} = \psi({g_2'}^{f(x)/x+e_i})$$

for $1 \leq i \leq q$. $\mathcal{A}$ is given $\mathsf{param} = (g_0, g_1, g_2, h_0, w, h, q_1, \ldots, q_{t_{max}})$. For simplicity, denote $e^* = e_q$.

Oracle Simulation. $\mathcal{B}$ simulates the extraction and signing oracles as follow:

(*Hash oracle.*) A new hash oracle query $H(ID)$ will return a new e_i that has never been returned by the hash oracle.

(*Extraction oracle.*) $\mathcal{S}$ runs the **Extract** protocol with $\mathcal{A}$, rewinds and extracts (s', r_s). For $i = 1, \ldots, q-1$, $\mathcal{S}$ randomly picks $s'' \in \mathbb{Z}_p^*$ and computes:

$$\begin{aligned} A &= (g_0 C g_2^{r_s})^{1/x+e_i} \\ &= (g_0^{1+r_s\mu+\frac{(s'+s'')[(e^*+x)k^*-1]}{a^*}})^{1/x+e_i} \\ &= A_i^{1+r_s\mu-\frac{(s'+s'')}{a^*}} g_0^{\frac{(s'+s'')k^*(e^*+x)}{a^*(e_i+x)}} \\ &= A_i^{(1+r_s\mu-\frac{(s'+s'')}{a^*})} \big(g_0^{\frac{(s'+s'')k^*}{a^*}}\big)^{(1-\frac{e_i-e^*}{e_i+x})} \\ &= A_i^{(1+r_s\mu-\frac{(s'+s'')}{a^*}-\frac{(s'+s'')k^*(e_i-e^*)}{a^*})} \big(g_0^{\frac{(s'+s'')k^*}{a^*}}\big) \end{aligned}$$

$\mathcal{S}$ returns (A, e_i, s'') to $\mathcal{A}$.

For $i = n$, $\mathcal{S}$ returns $(A_n = g_0^{k^*}, e_n, s'' = a^* - s')$ to $\mathcal{A}$.

(*Signing oracle.*) $\mathcal{S}$ uses the zero-knowledge simulator of the SPK in **Sign** to answer these queries.

Output Calculation. If $\mathcal{A}$ wins in the game in definition 8, $\mathcal{A}$ returns a signature σ_i^* for message m_i^* and ring L_i^* for $i = 0, 1$. Assume $\mathcal{A}$ wins by condition 1 of definition 8, then $\mathcal{A}$ must not query $\mathcal{KEO}$ for one ID^* before. WLOG, assume $\mathcal{A}$ didn't query for ID_0. $\mathcal{S}$ extract the witnesses (A, e, s, r_s, v_w) from the SPK in σ_i^*. These set of witnesses satisfies the following relationship based on the soundness of the SPK.

1. $A^{e+x} = g_0 g_1^s g_2^{r_s}$
2. $v_w^{e+q} = v$
3. $S = {u_0}^s$
4. $T = {u_0}^e u_1^{Rs}$

We have the following possibilities:

- Case 1: $e \notin \{e_1, \ldots, e_n\}$. Then $\mathcal{S}$ computes:

$$\begin{aligned} A^{e+x} &= g_0 g_1^s g_2^{r_s} = g_0^{1+r_s\mu+\frac{s[(e^*+x)k^*-1]}{a^*}} \\ A &= \big(g_0^{\frac{a^*+r_s\mu a^*-s}{a^*(e+x)}}\big)\big[\big(g_0^{\frac{sk^*}{a^*}}\big)^{(1-\frac{e-e^*}{e+x})}\big] \\ B &= \big(A g_0^{-\frac{sk^*}{a^*}}\big)^{\frac{a^*}{a^*+r_s\mu a^*-s-sk^*(e-e^*)}} \end{aligned}$$

  $\mathcal{S}$ returns (B, e) as a new SDH pair.
- Case 2: $e = e_i$ and $A \neq A_i$ for some i. With probability $1/q$, $e = e^*$, $\mathcal{S}$ computes as in case 1:

$$\begin{aligned} A &= \big(g_0^{\frac{a^*+r_s\mu a^*-s}{a^*(e+x)}}\big)\big(g_0^{\frac{sk^*}{a^*}}\big) \\ B &= \big(A g_0^{-\frac{sk^*}{a^*}}\big)^{\frac{a^*}{a^*+r_s\mu a^*-s}} \end{aligned}$$

  $\mathcal{S}$ returns (B, e) as a new SDH pair.

- Case 3: $e = e_i$ and $A_0 = A_i$ for some i. We must have $A_i^{e_i+x} g_1^{-s} g_2^{r_s} = A_i^{e_i+x} g_1^{-s_i} g_2^{r_{s_i}}$ which implies that $s + \mu r_s = s_i + \mu r_{s_i}$. If $\mathcal{A}$ wins in this situation, $\mathcal{S}$ can be set up easily to solve the DL of g_2 to base g_1 and thus this case happens with negligible probability under the DL assumption.

From the new SDH pair, we can solve the q-SDH problem. We have:

$$B = {g'_1}^{f(x)/(x+e)} = {g'_1}^{\sum_{i=0}^{q-1} c_i x^i + c_{-1}/(x+e)}$$

where $c_{-1}, c_0, \ldots, c_{q-1}$ can be computed by $\mathcal{S}$ with $c_{-1} \neq 0$. Then $\mathcal{S}$ get:

$${g'_1}^{1/(x+e)} = \big(B \prod_{i=0}^{q-1} \psi({g'_2}^{x^i})^{-c_i}\big)^{1/c_{-1}}$$

which is the solution to the q-SDH problem.

Now assume $\mathcal{A}$ wins by condition 2 of definition 8. If $ID' \notin \{L_0^* \cup L_1^*\}$, then it contradicts the soundness property of the SPK.

Thus, our construction is non-slanderable if DL assumption holds in $\mathbb{G}_p$ and q-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ in the random oracle model.