Identity-Based Ring Signature Schemes for Multiple Domains

JuHee Ki[1], Jung Yeon Hwang[2] and Dong Hoon Lee[3]
[1] Korea Evaluation Institute of Industrial Technology (KEIT), Daejeon, Korea
[2] Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea
[3] CIST, Korea University, Seoul, Korea
[e-mail: eye@keit.re.kr, videmot@etri.re.kr, donghlee@korea.ac.kr]
*Corresponding author: Dong Hoon Lee

Received March 30, 2012; revised June 30, 2012; accepted September 19, 2012
published October 29, 2012

Abstract

A separable identity-based ring signature scheme has been constructed as a fundamental cryptographic primitive for protecting user privacy. Using the separability property, ring members can be selected from arbitrary domains, thereby, giving a signer a wide range of ways to control privacy. In this paper we propose a generic method to construct efficient identity-based ring signature schemes with various levels of separability. We first describe a method to efficiently construct an identity-based ring signature scheme for a single domain, in which a signer can select ring identities by choosing from identities defined only for the domain. Next, we present a generic method for linking ring signatures constructed for a single domain. Using this method, an identity-based ring signature scheme with a compact structure, supporting multiple arbitrary domains can be designed. We show that our method outperforms the best known schemes in terms of signature size and computational costs, and that the security model based on the separability of identity-based ring signatures, presented in this paper, is highly refined and effective by demonstrating the security of all of the proposed schemes, using a model with random oracles.

Keywords: Identity-Based Ring Signature, Privacy, Anonymity, Separability, Multiple Domains

http://dx.doi.org/10.3837/tiis.2012.10.015

1. Introduction

Enabling ubiquitous applications most often requires a pervasive computing environment in which large amounts of user information are collected and distributed. In such environment, the risk of mistakenly collecting sensitive user data or willfully misusing user data is inherent. Therefore, in order to benefit from the convenience of information technology without running the risks associated with the proliferation of information, it is important that security procedures such as message authentication and user privacy protection should be properly implemented and followed. This paper deals with designing a separable identity-based ring signature (IBRS) scheme, which may be used as a basic primitive for security procedures.

The main purpose of a ring signature is to maintain an appropriate level of signer ambiguity and authenticate messages [1]. Using a list or a ring of arbitrary signers or ring members, a signer can generate a signature associated with the ring. A valid ring signature convinces the verifier that the signature has been generated by one of the members of the ring, without revealing the identity of the actual signer. Meanwhile, by applying identity-based cryptography to a ring signature scheme, one can simplify (certificate-based) public key management procedures. For example, an arbitrary public string such as an e-mail address or phone number may be used as a user's public key [2][3]. This technique for simplification of public key management is particularly suitable for ring signature schemes which deal with multiple signers (from the same domain) at a time, as it does not require additional certificates to associate random public keys with a user.

A domain can be defined using an identity-based signature (IBS) scheme. It should be noted that for a concrete implementation of an IBS scheme, specific public parameters and their corresponding master keys must be first generated and defined. A user obtains a private key for his or her identity, which is associated with the master private key. Then, according to the IBS scheme, signatures can be generated for message authentication and can be validated. Thus, a domain can be viewed as an instance of an IBS scheme, which is defined by a specific parameter. The same IBS scheme can have concrete instances that vary according to the master keys and parameters. On the other hand, in situations where two different IBS schemes are involved, the instances of the respective schemes will be always different.

An IBRS scheme can be devised only for a specific single domain by extending the structure of a particular IBS scheme that works in that domain [4], [5]. Realistically, however, it must be assumed that there are various domains that are based on various cryptographic techniques and assumptions. In order to achieve an appropriate level of privacy, an IBRS scheme must, therefore, be capable of supporting multiple domains; for example, a signer should be able to pick ring members arbitrarily from across various domains. This property allowing the selection of ring members from different domains is known as *separability*. Using the separability property, a signer can have fine-grained control over his/her privacy.

1.1 Our Contributions

In this paper, we propose a modular method which enables the efficient construction of IBRS schemes with varying levels of separability. To do this, we first present a basic method for constructing an efficient IBRS scheme for a single domain. We explain this method through concrete examples based on an RSA cryptosystem and pairing map parameters. Next, we present a generic method for constructing an IBRS scheme for multiple domains, using IBRS schemes designed for a single domain. The resulting IBRS schemes afford a high level of

separability, allowing, for example, a signer to select the identities of ring members from across different domains, irrespective of the public parameters and signing methods. Our method, extending the technique of [6], offers a good structure for linking various ID-based signatures sequentially. We present a highly-refined security model for a separable IBRS scheme and prove that all the proposed IBRS schemes achieve strong anonymity and unforgeability in the model. To demonstrate the effectiveness of our approach, we compare the performance of our schemes with that of other known IBRS schemes, with respect to the size of signatures and computational costs. Due to their intrinsic property of dealing with multiple (possible) signers at the same time, reducing the size of a signature is one of the critical efficiency concerns for IBRS schemes. We show that the signature size of our separable IBRS schemes is shorter than those of other known schemes with the same degree of separability.

1.2 Related Works

Since the first introduction of the notion of an identity-based cryptosystem by [2], many IBS schemes have been proposed using various cryptographic techniques based on RSA, discrete logarithm, or bilinear map parameters [3], [7][8][9][10]. [1], meanwhile, presented the concept of a non-ID-based ring signature scheme, proposing an RSA-based ring signature scheme. The first explicit construction of an IBRS scheme was presented by [11], and this scheme was without a formal security proof. Various other IBRS schemes have been suggested, subsequently, for improving efficiency or refining security models [4][12][13]. Some extensions of ring structures have been also presented to support a general access structure [4][14]. However, most IBRS schemes have thus far been constructed for single domains. Several works, including [6][13], and [15], have focused on a modular approach to combine signatures with different structures. The results by [6] and [15] provide novel methods to link non-ID-based signatures in a sequential or parallel manner. The result by [13] directly applied these link methods to ID-based signature schemes to achieve strong separability. Under the approach proposed in this study, as will be shown later in detail, signatures are significantly shorter in length, than those under the previously proposed approaches.

1.3 Organization

The rest of this paper is organized as follows: In section II, we present a security model for a separable IBRS scheme. In section III, we describe our IBRS scheme for a single domain and provide two instances of its use. In section IV, we present a generic method to construct an IBRS scheme for multiple domains, and prove the security of the IBRS scheme constructed using this method. In section V, we compare the size of our signatures to those of other best known signatures. Finally, we offer a conclusion in section VI.

2. Security Model

We formally define a security notion for a separable IBRS scheme. Let λ denote the fixed parameter for the size of user identities.

The notion of *separability* was introduced by [16] to quantify the amount of common system parameters for a signature. Levels of separability can be defined according to whether a pair of independent keys is used in a signature scheme or completely different signature schemes are in use. For example, when all parties must use the same signature scheme and

public system parameters, the level of separability is considered weak, while it is considered strong when parties may use potentially different signature schemes, and the signature is based on roughly the minimum security parameter of the signature schemes involved.

Next, we formally define a separable IBRS scheme Π, which consists of a tuple of polynomial-time algorithms, **SetUp**, **Extract**, **Sign**, and **Vrfy**.

- **SetUp** is a probabilistic polynomial-time (PPT) algorithm that, on input of security parameter κ, outputs a tuple of public system parameters $\pi = (\pi_1,\ldots, \pi_\alpha)$ and its corresponding master secret key $\text{msk} = (\text{msk}_1,\ldots, \text{msk}_\alpha)$, where α is a polynomial in κ.
- **Extract** is a PPT algorithm that, on input of msk_j, π_j, and $\text{ID} \in \{0,1\}^\lambda$, outputs a signing key $sk_{j,\text{ID}}$. This is denoted by $sk_{j,\text{ID}} \leftarrow$ **Extract** (msk_j, π_j, ID).
- **Sign** is a PPT algorithm that, on input of a private key $sk_{i,\text{ID}}$, a ring $\text{RID} = \{(\pi'_1, \mathbf{ID}_1),\ldots,(\pi'_n, \mathbf{ID}_n)\}$ for $\pi'_j \in \pi$ and $\mathbf{ID}_j = (\text{ID}_{j,1},\ldots, \text{ID}_{j,t[j]})$, and a message $m \in \{0,1\}^*$, outputs σ. Assume that i is selected in $\{1,\ldots,n\}$ uniformly at random, $\pi_i \in \{\pi'_1,\ldots,\pi'_n\}$ and $\text{ID} \in \mathbf{ID}_i$. This is denoted by $\sigma \leftarrow$ **Sign** ($sk_{i,\text{ID}}$, RID, m).
- **Vrfy** is a deterministic polynomial-time algorithm that, on input of π, a ring RID, message m, and signature σ, returns 1 (valid) or 0 (invalid). This is denoted by $b \leftarrow$ **Vrfy** (π, σ, RID, m).

In the above description, we assume that a signature scheme is implicitly defined or described in its corresponding public system parameter. Given that separability can be measured by α, when $\alpha = 1$, it represents the weakest level of separability; that is, a ring can be constructed by picking only users in the same domain. The greater the value of α, the greater the degree of separability. However, this is only a quantitatively measurement of separability and does not reflect qualitative separability. For example, the signature schemes corresponding to two different domain parameters π'_i and π'_j may be the same in some cases. To take this factor into consideration, we can measure separability using additional indices to indicate signature schemes in public system parameters π'_i. If the two system parameters π'_i and π'_j are defined for a signature scheme, we can assume that there is no increase in separability.

For security, an IBRS scheme must achieve correctness and two basic security notions, unforgeability and anonymity.

Correctness. We say that an IBRS scheme is correct if the following conditions hold: $1 \leftarrow$ **Vrfy** (π, σ, RID, m) for a message $m \in \{0,1\}^*$, a positive integer $n \in \text{N}$, and $\text{RID} = \{(\pi'_1,\mathbf{ID}_1),\ldots,(\pi'_n,\mathbf{ID}_n) \mid \pi'_i \in \pi, \mathbf{ID}_i = (\text{ID}_{i,1},\ldots, \text{ID}_{i,t[i]})\}$ where (msk, π) $\leftarrow$ **Setup** (1^κ); $sk_{i,\text{ID}} \leftarrow$ **Extract** (msk_i, π'_i, $\text{ID} \in \mathbf{ID}_i$); and $\sigma \leftarrow$ **Sign** ($sk_{i,\text{ID}}$, RID, m) for all $i = 1,\ldots,n$.

Unforgeability. An IBRS scheme Π is said to be *existentially unforgeable under adaptively chosen message and identity (CMIA) attacks* if no PPT adversary A has a non-negligible advantage in the following game with a challenger C.

(1) C runs **SetUp** to obtain $\pi = (\pi_1,\ldots,\pi_\alpha)$ and $\text{msk} = (\text{msk}_1,\ldots, \text{msk}_\alpha)$. The public parameters π is given to A.

(2) The adversary A adaptively makes polynomially many queries as follows.

- ***Extract*** query (π_j, ID): C returns $sk_{j,\text{ID}} \leftarrow$ **Extract** (msk_j, π_j, ID).

- ***Sign*** query $((\pi'_\beta, \mathrm{ID} \in \mathbf{ID}_\beta), \mathrm{RID}=\{(\pi'_1, \mathbf{ID}_1),\ldots,(\pi'_n, \mathbf{ID}_n)\}, m)$: C returns $\sigma \leftarrow$ **Sign** $(sk_{\beta,\mathrm{ID}}, \mathrm{RID}, m)$ where $sk_{\beta,\mathrm{ID}} \leftarrow$ **Extract** $(\mathrm{msk}_\beta, \pi'_\beta, \mathrm{ID})$.

(3) A outputs $\mathrm{RID}^*=\{(\pi^*_1,\mathbf{ID}^*_1),\ldots,(\pi^*_n,\mathbf{ID}^*_n)\}$, m^*, and σ^*.

A succeeds in the game if σ^* on (m^*, RID^*) is valid, i.e., $1 \leftarrow$ **Vrfy** $(\pi, \sigma^*, \mathrm{RID}^*, m^*)$ and for all j=1,...,n, **Extract** $(\mathrm{msk}^*_j, \pi^*_j, \mathrm{ID}^* \in \mathbf{ID}^*_j)$ and **Sign** $((\pi^*_j, \mathrm{ID}^* \in \mathbf{ID}^*_j), \mathrm{RID}^*, m^*)$ queries have never been issued. A successful event is denoted by $\mathrm{Suc}_{\mathrm{forg}}$. The EUF-advantage of A for Π is defined by $\mathrm{Adv}^{\mathrm{IBRS,\ EUF\text{-}CMIA}}(\Pi,A) = \Pr[\mathrm{Suc}_{\mathrm{forg}}]$.

Anonymity - An IBRS scheme Π is said to be *anonymous* if no PPT adversary A has a non-negligible advantage in the following game with a challenger C.

(1) C runs **SetUp** to obtain $\pi = (\pi_1, \ldots, \pi_\alpha)$ and msk. The public parameters π is given to A.

(2) The adversary A adaptively makes polynomially many queries as follows.

- ***Extract*** query (π_j, ID): C returns $sk_{j,\mathrm{ID}} \leftarrow$ **Extract** $(\mathrm{msk}_j, \pi_j, \mathrm{ID})$.
- ***Sign*** query $((\pi'_\beta, \mathrm{ID} \in \mathbf{ID}_\beta), \mathrm{RID}=\{(\pi'_1, \mathbf{ID}_1),\ldots,(\pi'_n, \mathbf{ID}_n)\}, m)$: C returns $\sigma \leftarrow$ **Sign** $(sk_{\beta,\mathrm{ID}}, \mathrm{RID}, m)$.

(3) The adversary A outputs a message m^*, two distinct tuples of a public parameter and an identity, $((\pi^*_0, \mathrm{ID}^*_0), (\pi^*_1, \mathrm{ID}^*_1))$, and a ring RID^* for which $(\pi^*_0, \mathrm{ID}^*_0), (\pi^*_1, \mathrm{ID}^*_1) \in \mathrm{RID}^*$, and $\pi^*_0, \pi^*_1 \in \pi$.

(4) The challenger C picks a random bit $b \in \{0,1\}$ and gives A with the signature on $\mathrm{ID}=\mathrm{ID}^*_b$, $\sigma' \leftarrow$ **Sign**$(sk_{b,\mathrm{ID}}, \mathrm{RID}^*, m^*)$.

(5) A makes ***Extract*** and ***Sign*** queries adaptively.

(6) Finally, the adversary outputs bit b'.

A succeeds in the game if $b = b'$. The successful event is denoted by $\mathrm{Suc}_{\mathrm{anon}}$. The ANON-advantage of A for Π is defined by $\mathrm{Adv}^{\mathrm{IBRS,\ Anon\text{-}CMIA}}(\Pi,A) = \Pr[\mathrm{Suc}_{\mathrm{anon}}]$.

The above definition considers anonymity against full key exposure; that is, an adversary can obtain the secret keys of all honest users including even users in the ring. As noted by [12], this definition is polynomial-time equivalent to the case in which an adversary should be unable to guess the real signer among r, randomly chosen ring members, with probability better than $1/r + \varepsilon$ for a negligible ε.

3. IBRS Schemes for a Single Domain

In this section, we present an efficient method of extending IBS schemes into IBRS schemes for a single domain. Throughout the paper, we denote by $\oplus$ and || bitwise-eXclusive OR and concatenation operations, respectively. Meanwhile, we denote by $\Phi(N)$ Euler's totient function. We define $\oplus_{i=1,\ldots,k} c_i = c_1 \oplus \ldots \oplus c_k$ for L-bit strings $c_i \in \{0,1\}^L$.

Intuitively, the main idea of our construction is to aggregate random commitments for other fake signers into a single random commitment using a common public system parameter. Since a real signer can compute a secret share in advance, he/she can generate a correct response using his/her signing key, the secret share, and a random number. The response can

be used to cancel exactly the identity of the real signer in the verification equation without changing the aggregated commitment. In the process, the identity of the signer is not exposed thanks to the computational symmetry of the verification equation. Our method is as follows where the choice of domains is not considered, as the scheme is constructed for one particular domain:

- **SetUp.** Given a security parameter κ, output a *master secret key* msk and its corresponding public system parameters π. Assume that π includes a cryptographic hash function $H:\{0,1\}^* \rightarrow \{0,1\}^L$.
- **Extract.** Given an identity ID, return its corresponding private key sk_{ID}.
- **Sign.** Given π, a signing key sk_{ID}, message m, and a ring of identities $RID=(\pi, (ID_1,\ldots,ID_t))$ including $ID=ID_\beta$ for random $\beta \in \{1,\ldots,t\}$, pick random $c_i \in \{0,1\}^L$ for $i=1,...,t$, $(i \neq \beta)$, and some randomness R_β and compute a simulated commitment B. This is denoted by $B \leftarrow \textbf{\textit{Sim}}(\pi, RID, R_\beta, (c_1,...,c_{\beta-1},c_{\beta+1},...,c_t))$. Compute a challenge $w \leftarrow H(RID, m, B)$. Also compute $c_\beta = w \oplus (\oplus_{i=1,\ldots,t,\ (i \neq \beta)} c_i)$ and a response V using share c_β, randomness R_β, and signing key sk_{ID}. Output $\sigma = (c_1,...,c_t,V)$.
- **Vrfy.** Given π, a ring RID, message m, and $\sigma = (c_1,...,c_t,V)$, compute $B' \leftarrow \textbf{\textit{VComp}}(\pi, RID, c_1,...,c_t,V)$ and check if $c_1 \oplus \ldots \oplus c_t = H(RID, m, B')$. If the equality holds, then output 1; otherwise output 0.

For correctness, it is required that $\textbf{\textit{Sim}}\ (\pi, RID, R_\beta, (c_1,...,c_{\beta-1}, c_{\beta+1},..., c_t) = \textbf{\textit{VComp}}\ (\pi, RID, c_1,...,c_t, V)$.

To explain our method through concrete examples, we chose two IBRS schemes extending the RSA-based IBS [7] and (modified) pairing-based IBS [8] schemes, respectively. The first RSA-based IBRS scheme is as follows:

- **SetUp.** Given a security parameter κ, generate two random λ_0-bit primes p_1, p_2 and compute $N = p_1p_2$. Let $L \leq \lambda_0$. Select $e \in \{0,1\}^L$ such that $\gcd(\Phi(N),e) = 1$. Let $d = e^{-1} \bmod N$. Generate cryptographic hash functions $H_{id} : \{0,1\}^\lambda \rightarrow Z_N^*$ and $H: \{0,1\}^* \rightarrow \{0,1\}^L$. Output a *master secret key* $msk = (p_1,p_2)$ and a public system parameter $\pi = (N, e, H_{id}, H)$.

- **Extract.** Given an identity ID, compute $Q = H_{id}(ID)$ and $sk_{ID} = Q^d \bmod N$, and return sk_{ID}. If $sk_{ID}^e = H_{id}(ID) \bmod N$, then sk_{ID} is a valid key for the ID.

- **Sign**. Given π, a signing key sk_{ID}, message m, and a ring $RID = (\pi, (ID_1,\ldots,ID_t))$, including $ID = ID_\beta$, select random $r \in Z_N^*$, $c_i \in \{0,1\}^L$ for $i=1,...,t$, $(i \neq \beta)$ and compute $Q_i = H_{id}(ID_i)$, $B=r^e \Pi_{i=1,\ldots,t,(i\neq\beta)} Q_i^{c_i} \bmod N$, $w = H(RID, m, B)$, $c_\beta = w \oplus (\oplus_{i=1,\ldots,t,(\ i \neq \beta)} c_i)$, $V=r \cdot (sk_{ID})^{-c_\beta} \bmod N$. Output $\sigma = (c_1,...,c_t,V)$.

- **Vrfy.** Given π, a ring RID, message m, and $\sigma = (c_1,...,c_t,V)$, check if $c_1 \oplus ... \oplus c_t = \mathrm{H}(\mathrm{RID}, m, V^e \cdot \Pi_{i=1,...,t} Q_i^{c_i} \bmod N)$ where $Q_i = \mathrm{H_{id}}(\mathrm{ID}_i)$. If the equality holds, then output 1; otherwise output 0.

It is easy to see that the above IBRS scheme is correct, because $c_1 \oplus ... \oplus c_t = w = \mathrm{H}(\mathrm{RID}, m, B) = \mathrm{H}(\mathrm{RID}, m, r^e \Pi_{i=1,...,t\,(i\neq\beta)} Q_i^{c_i} \bmod N) = \mathrm{H}(\mathrm{RID}, m, ((Q_\beta^d)^{c_\beta} \cdot r)^e Q_\beta^{c_\beta} \Pi_{i=1,...,t\,(i\neq\beta)} Q_i^{c_i} \bmod N) = \mathrm{H}(\mathrm{RID}, m, V^e \cdot \Pi_{i=1,...,t} Q_i^{c_i} \bmod N)$.

Theorem 1. Let $\mathrm{H_{id}}$ and H be random hash functions. The above RSA-based IBRS scheme is anonymous against full key exposure.

Proof. A simulator sets up all parameters correctly as defined in the proposed IBRS scheme. All private keys $sk_{\mathrm{ID}} = \mathrm{H_{id}}(\mathrm{ID})^d \bmod N$ are given to an adversary. A simulator can provide a perfect simulation with the adversary because it knows all private keys. As in the definition of anonymity in section II, assume that an adversary outputs two distinct identities ID_1 and ID_2 for the proposed IBRS scheme. Since the scheme is constructed for a single domain we do not consider the choice of domains.

For random $b \in \{0,1\}$, assume that signature $\sigma = (c_0, c_1, V)$ is generated according to the signing method of the proposed IBRS scheme. That is, for a given signing key $sk_{\mathrm{ID},b} = \mathrm{H_{id}}(\mathrm{ID}_b)^d$, message m, and ring of identities $\mathrm{RID} = (\pi, (\mathrm{ID}_0, \mathrm{ID}_1))$, select random $r \in \mathrm{Z_N}^*$ and $c_z \in \{0,1\}^{\mathrm{L}}$ for $z\,(\neq b) \in \{0,1\}$ and then compute $Q_{\mathrm{ID},z} = \mathrm{H_{id}}(\mathrm{ID}_z)$, $B = r^e Q_z^{c_z} \bmod N$, $w = \mathrm{H}(\mathrm{RID}, m, B)$, $c_b = w \oplus c_z$, $V = r \cdot (sk_{\mathrm{ID},b})^{-c_b} \bmod N$. Note that $c_0 \oplus c_1 = \mathrm{H}(\mathrm{RID}, m, V^e \cdot Q_0^{c_0} \cdot Q_1^{c_1})$. The verification equation shows the symmetry of computation with respect to identity. In fact, $V = r \cdot (sk_{\mathrm{ID},b})^{-c_b}$ can be equivalently represented by $V = r' \cdot (sk_{\mathrm{ID},z})^{-c_z}$, where $r' = r \cdot (sk_{\mathrm{ID},z})^{c_z} \cdot (sk_{\mathrm{ID},b})^{-c_b}$, while maintaining the validity of the signature. Also, r' is uniformly distributed over Z_N^* because r is uniformly distributed over Z_N^*, and r' is represented by a linear combination of fixed parameters $sk_{\mathrm{ID},z}$, $sk_{\mathrm{ID},b}$, c_z, and c_b. This means that V can be generated equally by a key for ID_0 or ID_1, though it was generated by the key for a specific identity.

Therefore, for given (m, RID, σ), the probability that a specific ID_i in RID is the identity of the real singer is 1/2. □

Theorem 2. Let $\mathrm{H_{id}}$ and H be random hash functions. The above RSA-based IBRS scheme is existentially unforgeable under CMIA attacks under the hardness of the RSA problem.

Proof. We show that the security of the proposed IBRS scheme is reduced to the hardness of the RSA problem. We want to build an algorithm A that uses a forger F against our IBRS scheme to solve the RSA problem. Suppose that a random RSA instance (N, e, y) is given to A. Its goal is to compute x such that $x^e = y \bmod N$.

A gives system parameters $\pi = (N, e)$ to F. A simulates oracle queries as follows: Suppose F makes at most q_{id} and q_{H} queries to $\mathbf{H_{id}}$ and $\mathbf{H}$ oracles, respectively. For simplicity, we also assume that hash-queries are never repeated.

- $\mathbf{H_{id}}$ query. First, A chooses $\theta \in \{1,\ldots, q_{\mathrm{id}}\}$ uniformly at random. On an $\mathbf{H_{id}}(\mathrm{ID}_i)$ query, if it is the θ^{th} $\mathbf{H_{id}}$ query, let $\mathrm{ID}_i = \mathrm{ID}^*$. A returns y. Otherwise, A picks a random $D \in \mathrm{Z_N}^*$ and returns $D^e \bmod N$.

- **H** query. *A* obviously responds as follows: On a query, *A* picks random $w \in \{0,1\}^L$ and returns *w*.
- ***Extract*** query. On an ***Extract***(ID) query, if $ID \neq ID^*$ then *A* returns $sk_{ID} = D$ for $H_{id}(ID) = D^e \bmod N$. Otherwise, *A* outputs FAIL and aborts the simulation.
- ***Sign*** query. On a ***Sign*** $(ID_x, RID=(\pi, (ID_1,\ldots,ID_t)), m)$ query, if $ID_x \neq ID^*$, then *A* returns σ after correctly generating a signature σ with the signing key for ID_x. Otherwise, *A* chooses $c_1,...,c_t \in \{0,1\}^L$ and $V \in Z_N^*$ uniformly at random. Then, *A* computes $Y = V^e \cdot \Pi_{i=1,\ldots,t} H_{id}(ID_i)^{c_i} \bmod N$. Define $h = c_1+...+c_t$ as the value of H(RID, *m*, *Y*). *A* returns $\sigma = (c_1,...,c_t,V)$.

Eventually, *F* outputs a valid ring signature $\sigma^* = (c'_1,...,c'_s,V')$ on (RID^*, m^*), where $RID^* = (\pi, (ID^*_1,...,ID^*_s))$. Assume that for all $j = 1,...,s$, ***Extract*** (ID^*_j) and ***Sign*** (ID^*_j, RID^*, m^*) queries have never been issued. Let $Y' = V'^{e} \cdot \Pi_{i=1,\ldots,s} H_{id}(ID^*_i)^{c'_i} (\bmod N)$ and $h' = H(RID^*, m^*, Y')$.

By using a standard rewinding technique, we can non-negligibly obtain another forged signature $\sigma^{**} = (c''_1,...,c''_s,V'')$ satisfying the following condition: $h' \neq h''$,where $Y'' = V''^{e} \cdot \Pi_{i=1,\ldots,s} H_{id}(ID^*_i)^{c''_i} (\bmod N)$ and $h'' = H(RID^*, m^*, Y'')$. For some $\beta \in \{1,...,s\}$, $c'_\beta \neq c''_\beta$ and $c'_j = c''_j$ for $j = 1,...,s$ $(j \neq \beta)$.

If $ID_\beta = ID^*$ then *A* can compute $Z = V'(V'')^{-1} = x^\xi$ for $\xi = -c'_\beta + c''_\beta$. As already noted in the proof of Theorem 1, due to the symmetry of the verification equation, $V' = r \cdot (sk_{ID^*})^{-c'_\beta}$ for some $r \in Z_N^*$. In addition, by the condition of the rewinding technique, we have $V'' = r \cdot (sk_{ID^*})^{-c''_\beta}$. Thus, we can have $Z = V'(V'')^{-1} = r \cdot (sk_{ID^*})^{-c'_\beta} (r \cdot (sk_{ID^*})^{-c''_\beta})^{-1} = x^\xi$, where $\xi = -c'_\beta + c''_\beta$. Using a similar method, *A* can compute another $Z' = V'' \cdot (V''')^{-1} = x^{\xi'}$, where $\xi' = -c''_\beta + c''''_\beta$. Next, *A* computes integers τ and τ' such that $\tau\xi + \tau'\xi' = 1$ using the extended Euclidean algorithm. Finally, *A* outputs $T = Z^\tau \cdot (Z')^{\tau'} = x^{\xi\tau} \cdot x^{\xi'\tau'} = x^{\xi\tau + \xi'\tau'} = x = y^d \bmod N$ as a solution to the given RSA problem.

It is well-known that the probability that two random numbers are relatively prime is $6/\pi^2 \approx 0.6$ [17]. Hence *A* can highly compute τ and τ'. It is easy to see that the simulation that *A* makes is perfect unless an abortion occurs. The adversary *A* does not abort the simulation if *A* at least correctly guesses the value of θ, i.e, $ID_\theta = ID^* = ID_\beta$. Since ID^* is uniformly selected from the viewpoint of the forger, the probability of the event is at least $1/q_{id}$. Therefore, if the forger *F* who can break our IBRS scheme exists, then a poly-time solver to the RSA problem in G_1 non-negligibly exists. □

The second pairing-based IBRS scheme is described as follows.

- **SetUp**. Given a security parameter κ, generate an admissible bilinear map **e**: $G_1 \times G_2 \rightarrow G_T$, a random generator *P* of G_1. Pick a random $s \in Z_q^*$ and compute $P_{pub} = sP$. Let $\pi = (\mathbf{e}, G_1, G_2, G_T, q, P, P_{pub}, H_{id}, H)$, where $H_{id}: \{0,1\}^\lambda \rightarrow G_1$ and $H: \{0,1\}^* \rightarrow Z_q^*$ are cryptographic hash functions. Output a *master secret key* msk=*s* and public system parameters π.

- **Extract**. Given an identity ID, compute $Q = H_{id}(ID)$ and return the private key $sk_{ID} = sQ \in G_1$.

- **Sign**. Given π, a signing key sk_{ID}, message m, and a ring of identities RID = (π, ($ID_1,\ldots,ID_t$)), including ID = ID_β, select random $r \in Z_q^*$ and $c_i \in \{0,1\}^L$ for $i = 1,...,t$, ($i \neq \beta$). Then, compute $Q_i = H_{id}(ID_i)$, $B = rQ_\beta + \sum_{i=1,\ldots,t\ (i\neq\beta)} c_iQ_i \in G_1$, $w = H(RID, m, \mathbf{e}(B,P_{pub}))$, $c_\beta = w \oplus (\oplus_{i=1,\ldots,t,\ (i\neq\beta)} c_i)$, $V = (-c_\beta+r)\cdot sk_{ID} \in G_1$. Output $\sigma = (c_1,...,c_t,V)$.

- **Vrfy**. Given π, a ring RID, message m, and $\sigma = (c_1,...,c_t,V)$, compute $D' = \mathbf{e}(V,P)\cdot\mathbf{e}(\sum_{i=1,\ldots,t} c_iQ_i, P_{pub})$ and check if $c_1 \oplus \ldots \oplus c_t = H(RID, m, D')$, where $Q_i = H_{id}(ID_i)$. If the equality holds, then output 1; otherwise output 0.

It is easy to see that the above IBRS scheme is correct because $\mathbf{e}(B,P_{pub}) = \mathbf{e}(rQ_\beta+\sum_{i=1,\ldots,t(i\neq\beta)} c_iQ_i, P_{pub}) = \mathbf{e}((r-c_\beta)Q_\beta + \sum_{i=1,\ldots,t} c_iQ_i,P_{pub}) = \mathbf{e}(V,P) \cdot \mathbf{e}(\sum_{i=1,\ldots,t} c_i\ Q_i, P_{pub})$.

Theorem 3. Let H_{id} and H be random hash functions. The above pairing-based IBRS scheme is unconditionally anonymous against full key exposure.

Proof. A simulator sets up all parameters correctly as defined in the proposed IBRS scheme. All private keys $sk_{ID} = sH_{id}(ID) \in G_1$ are given to the adversary. A simulator can provide a perfect simulation to the adversary because it knows all of the private keys. As in the definition of anonymity in section II, assume that the adversary outputs two distinct identities, ID_1 and ID_2, for the proposed IBRS scheme. Since the scheme is constructed for a single domain, we do not consider the choice of domains.

For a random $b \in \{0,1\}$, assume that a signature $\sigma = (c_0, c_1, V)$ is generated according to the signing method of the proposed IBRS scheme. That is, given a signing key $sk_{ID,b} = sH_{id}(ID_b)$, message m, and a ring RID = (π, (ID_0, ID_1), select random $r \in Z_q^*$ and $c_z \in \{0,1\}^L$ and then compute $Q_z = H_{id}(ID_z)$, $B = r\ Q_b + c_z\ Q_z \in G_1$, $w = H(RID, m, \mathbf{e}(B, P_{pub}))$, $c_b = w \oplus c_z$, $V = (-c_b+r)\cdot sk_{ID,b} \in G_1$.

By the definition of the verification algorithm, it holds that $c_0 \oplus c_1 = H(RID, m, \mathbf{e}(V,P)\cdot\mathbf{e}(c_0Q_0+c_1Q_1,P_{pub}))$. The verification equation has computational symmetry with respect to an identity. In fact, $V = (-c_b + r) \cdot sk_{ID,b}$ can be equivalently represented by $V = (-c_z + r')\cdot sk_{ID,z}$, where $r' = c_z + (r - c_b)\cdot\alpha$ and $sk_{ID,b} = \alpha \cdot sk_{ID,z}$ for some $\alpha \in Z_q^*$. Note that $V = (-c_z + r')\cdot sk_{ID,z} = (-c_z + c_z + (r - c_b)\cdot\alpha)\cdot sk_{ID,z} = (r - c_b)\cdot sk_{ID,b}$. Here, r' is uniformly distributed over G_1 because r is uniformly distributed over G_1, and r' is represented by a linear combination of fixed parameters α, c_z and c_b. This means that V can be generated equally by a key for ID_1 or ID_2, although it was generated by the key for a specific identity.

Therefore, for given (m, RID, σ), the probability that a specific ID_i in RID is the identity of the real singer is 1/2. □

Theorem 4. Let H_{id} and H be random hash functions. The above pairing-based IBRS scheme is existentially unforgeable under CMIA attacks under the hardness of the computational DH problem.

Proof. We want to build an algorithm *A* that uses a forger *F* against our pairing-based IBRS scheme to solve the CDH problem. Suppose that a random CDH instance (P, $\mathbf{A} = \alpha P$, $\boldsymbol{B} = \beta P$) is given to *A*. Its goal is to compute $\alpha\beta P \in G_1$. *A* sets $P_{pub} = \mathbf{A}$ (= αP) and gives system parameters $\pi = (\mathbf{e}, G_1, G_2, G_T, q, P, P_{pub})$ to *F*. *A* simulates the oracle queries as follows: Suppose *F* makes at most q_{id} and q_H queries to H_{id} and H oracles, respectively. For simplicity, we also assume that hash-queries are never repeated.

- **H_{id}** query. First, *A* chooses $\theta \in \{1,\ldots,q_{id}\}$ uniformly at random. On an H_{id}(ID) query, if it is the θ^{th} H_{id} query, let ID = ID^*. *A* returns $\mathbf{B} = \beta P$; otherwise, *A* picks a random $z \in Z_q^*$ and returns zP.
- **H** query. *A* obviously responds as follows: On a query, *A* picks random $w \in \{0,1\}^L$ and returns *w*.
- ***Extract*** query. On an ***Extract*** (ID) query, if ID ≠ ID^*, then *A* returns $sk_{ID} = zP_{pub}$ using *z* with H_{id} (ID) = zP. Otherwise, *A* outputs FAIL and aborts the simulation.
- ***Sign*** query. On a ***Sign*** (ID_x, RID =(π, ($ID_1,\ldots,ID_t$)), *m*) query, if $ID_x \neq ID^*$, then *A* returns σ after correctly generating a signature σ with the signing key for ID_x. Otherwise, *A* chooses $c_1,\ldots,c_t \in Z_q^*$ and $V \in G_1$ uniformly at random. Then, *A* computes $Y = \mathbf{e}(V,P) \cdot \mathbf{e}(\sum_{i=1,\ldots,t} c_i H_{id}(ID_i), P_{pub})$. Define $h = c_1+\ldots+c_t$ as the value of H(RID, *m*, *Y*). *A* returns $\sigma = (c_1,\ldots,c_t,V)$.

Eventually, *F* outputs a valid ring signature $\sigma^* = (c'_1,\ldots,c'_s,V')$ on (RID^*, m^*), where $RID^* = (\pi, (ID^*_1,\ldots,ID^*_s))$. Assume that for any ID$\in\{ID^*_1,\ldots,ID^*_s\}$, ***Extract***(ID) and ***Sign***(ID, RID^*, m^*) queries have never been issued. Let $Y' = \mathbf{e}(V',P) \cdot \mathbf{e}(\sum_{i=1,\ldots,s} c'_i H_{id}(ID^*_i), P_{pub})$ and $h' = H(RID^*, m^*, Y')$.

By using a rewinding technique, we can non-negligibly obtain another forged signature $\sigma^{**} = (c''_1,\ldots,c''_s,V'')$ satisfying the following condition: $h' \neq h''$ where $Y'' = \mathbf{e}(V'',P) \cdot \mathbf{e}(\sum_{i=1,\ldots,s} c''_i H_{id}(ID^*_i), P_{pub})$ and $h'' = H(RID^*, m^*, Y'')$. For some $\beta \in \{1,\ldots,s\}$, $c'_\beta \neq c''_\beta$ and $c'_j = c''_j$ for $j = 1,\ldots,s$ ($j \neq \beta$).

Note that if $ID_\beta = ID^*$, then the algorithm *A* can compute $Z = (-c'_\beta + c''_\beta)^{-1}(V' - V'') = sk_{ID^*} = \alpha\beta P$ as a solution to the given CDH instance. As already noted in the proof of Theorem 3, due to the symmetry of the verification equation, $V' = (-c'_\beta + r) \cdot sk_{ID^*}$ for some $r \in Z_q^*$. In addition, by the condition of the rewinding technique, we can have $V'' = (-c''_\beta + r) \cdot sk_{ID^*}$. Thus, we have $Z = (-c'_\beta + c''_\beta)^{-1}(V' - V'') = (-c'_\beta + c''_\beta)^{-1}[(-c'_\beta + r) \cdot sk_{ID^*} - (-c''_\beta + r) \cdot sk_{ID^*}] = sk_{ID^*} = \alpha H_{id}(ID^*) = \alpha\beta P$.

It is easy to see that the simulation that *A* makes is perfect unless an abortion occurs. The adversary *A* does not abort the simulation if *A* correctly guesses at least the value θ, i.e, $ID_\theta = ID^* = ID_\beta$. Since ID^* is uniformly selected from the viewpoint of the forger, the probability of the event is at least $1/q_{id}$. Therefore, if a forger *F* who can break our IBRS scheme exists, then a poly-time solver to the CDH problem in G_1 non-negligibly exists. □

4. A Generic Construction for IBRS Schemes for Multiple Domains

We present a generic method to construct an IBRS scheme for multiple domains from IBRS schemes for a single domain. The resulting IBRS schemes achieve strong separability; a signer can, for example, select identities from across different master-key domains, regardless of public parameters or signing methods. Our method basically extends the technique of [6] for linking signatures with different structures. It should be noted that the technique has a good structure for accommodating various proof-of-knowledge schemes sequentially. However, the technique cannot be directly applied to IBRS schemes for single domains because it was originally devised to link non-identity-based signatures. Also, this will necessitate the simultaneous treatment of multiple challenges for generating an IBRS . For our purposes, we modify the technique using a simple (t,t) secret sharing method.

1. Our Extension Method

Let us describe our extension method more concretely. Let $\pi = (\pi_1,...,\pi_\alpha)$ and $\Sigma_i = (\mathbf{Extract}_i, \mathbf{Sign}_i, \mathbf{Vrfy}_i)$ be an IBRS scheme for single domains, which can be generically constructed, as shown in the previous section. Assume that π_j includes a cryptographic hash function H_j: $\{0,1\}^* \rightarrow \{0,1\}^{L_j}$. Here, Σ_i is assumed to be defined with each domain parameter π_i. We assume that each $ID_{i,j}$ is associated with a master-key domain, π_i, and is included in $\mathbf{ID}_i = (ID_{i,1},\ldots, ID_{i,t[i]})$ for a positive integer $t[i]$. We also assume that a real signer with an identity, $ID_{\beta,\gamma} \in \mathbf{ID}_\beta$, in domain π_β obtains a secret signing key $sk_{\beta,\gamma}$ from the $\mathbf{Extract}_\beta$ algorithm.

- **Sign.** Given π, a secret signing key $sk_{\beta,\gamma}$, message m, and a ring $RID=\{(\pi'_1,\mathbf{ID}_1),\ldots,(\pi'_n,\mathbf{ID}_n) | \ \pi'_j \in \pi\}$ for random $\beta \in \{1,\ldots,n\}$ and $\gamma \in \{1,\ldots,t_{[\beta]}\}$, perform the following:
  - ***Initialization***. First, pick random $c_{\beta,i} \in \{0,1\}^{L_\beta}$ for $i=1,...,t_{[\beta]}$, $(i\neq\gamma)$ and randomness R_β, and compute a simulated commitment $B_\beta \leftarrow \boldsymbol{Sim}(\pi_\beta, \text{RID}, R_\beta, (c_{\beta,1},...,c_{\beta,\gamma-1},c_{\beta,\gamma+1},...,c_{\beta,t[\beta]}))$. Compute a challenge $w_{\beta+1} \leftarrow H_{\beta+1}(\text{RID}, m, B_\beta)$.
  - ***Simulation***. For each $j=\beta+1,...,n,1,...,\beta-1$, ① pick random $c_{j,i} \in \{0,1\}^{L_j}$ for $i = 2,...,t_{[j]}$ and then compute the challenge share $c_{j,1} = w_j \oplus (\oplus_{i=2,\ldots,t[j]} c_{j,i})$, ② pick a random V_j and compute $B_j \leftarrow \boldsymbol{VComp}(\pi_j, \text{RID}, c_{j,1},...,c_{j,t[j]}, V_j)$, and ③ compute $w_{j+1} \leftarrow H_{j+1}(\text{RID}, m, B_j)$.
  - ***Real Proof***. Compute $c_{\beta,\gamma} = w_\beta \oplus (\oplus_{j=1,\ldots,t[j]\ (j\neq\gamma)} c_{\beta,j})$ and response V_β using the signing key, $sk_{\beta,\gamma}$, R_β, and $c_{\beta,\gamma}$.

Output signature $\sigma = \{(c_{j,1},...,c_{j,t[j]},V_j) | \ 1 \le j \le n\}$ for positive integers $t[j]$.

- **Vrfy**. Given π, a message m, ring RID, and a signature $\sigma = \{(c_{j,1},...,c_{j,t[j]},V_j) | \ 1 \le j \le n\}$, for each $j = 1,...,n$, compute $B'_j \leftarrow \boldsymbol{VComp}(\pi_j, \text{RID}, c_{j,1},...,c_{j,t[j]}, V_j)$ and then check if $\oplus_{i=1,\ldots,t[j+1]} c_{j+1,i} = H_{j+1}(\text{RID}, m, B'_j)$. If all the equalities hold then output 1; otherwise, output 0.

Assume that the given underlying IBRS schemes used for the domain are correct, that is, for $\gamma \in \{1,...,t_{[j]}\}$, $\boldsymbol{Sim}(\pi_\beta, \text{RID}, R_{\beta,\gamma}, (c_{\beta,1},...,c_{\beta,\gamma-1},c_{\beta,\gamma+1},...,c_{\beta,t[\beta]}) = \boldsymbol{VComp}(\pi_\beta, \text{RID}, c_{\beta,1},...,c_{\beta,t[\beta]}, V_\beta)$. Using the assumption, we can show as follows that the extended IBRS scheme is correct: For j $(\neq\beta)$, by construction, w_j is computed in the signing and verifying algorithms using the same value B_j. For $j=\beta$, by correctness of a given underlying IBRS scheme, $\boldsymbol{Sim}(\pi_j, \text{RID}, R_{j,\gamma},$

$(c_{j,1},...,c_{j,\gamma-1}, c_{j,\gamma+1},...,c_{j,t[j]})) = B_j =$ ***VComp*** $(\pi_j, \text{RID}, c_{j,1},...,c_{j,t[j]}, V_j)$, and so the same hash value w_j is computed from B_j in the signing and verifying algorithms.

Next, we show that if the underlying IBRS schemes for single domains are secure, the extended scheme for multiple domains is secure in the random oracle.

Theorem 5. The extended IBRS scheme is anonymous against full key exposure if the underlying IBRS schemes used for the domain are anonymous against full key exposure in the random oracle model.

Proof. First, consider a case in which two identities, say $\text{ID}_{\theta,1}$ and $\text{ID}_{\theta,2}$, are selected in a domain. In this case, it is easy to see that the anonymity of the extended scheme is reduced to that of the underlying scheme used for the domain. Hence, the extended scheme is anonymous against full key exposure because, by assumption, the underlying scheme is anonymous against full key exposure.

Second, consider a case in which two identities are selected in two different domains, π_θ and π_ω. Denote the identities by $\text{ID}_{\theta,1}$ and $\text{ID}_{\omega,1}$, respectively. For simplicity, we assume that RID = $\{(\pi_\theta, \text{ID}_{\theta,1}), (\pi_\omega, \text{ID}_{\omega,1})\}$ is a ring that the adversary selects. Consider two distributions of signatures, D_θ and D_ω, where D_θ (resp. D_ω) is a distribution of signatures that a real signer in the domain π_θ (resp. π_ω) generates. Consider a signature $\sigma = \{(c_{1,1},V_1), (c_{2,1},V_2)\} \in \text{D}_\theta$. By the construction, $c_{1,1} = \text{H}_1(\text{RID}, m,$ ***VComp***$(\pi_\omega, \text{RID}, c_{2,1}, V_2))$ and $c_{2,1} = \text{H}_2(\text{RID}, m,$ ***Sim***$(\pi_\theta, \text{RID}, R_1))$. Because of the correctness of the underlying IBRS scheme, we also have ***Sim*** $(\pi_\theta, \text{RID}, R_1) =$ ***VComp***$(\pi_\theta, \text{RID}, c_{1,1}, V_1)$, and so $c_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c_{1,1}, V_1))$. Since the random hash model is considered in the proof, $c_{1,1}$ and $c_{2,1}$ are uniformly distributed.

Next, consider another case, that is, a signature $\sigma' = \{(c'_{1,1},V'_1), (c'_{2,1},V'_2)\} \in \text{D}_\omega$. We have $c'_{1,1} = \text{H}_1(\text{RID}, m,$ ***Sim***$(\pi_\omega, \text{RID}, R'_2))$ and $c'_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c'_{1,1}, V'_1))$. Because of the correctness of the underlying IBRS scheme, we have ***Sim*** $(\pi_\omega, \text{RID}, R'_2) =$ ***VComp***$(\pi_\omega, \text{RID}, c'_{2,1}, V'_2)$, and thus $c'_{1,1} = \text{H}_1(\text{RID}, m,$ ***VComp***$(\pi_\omega, \text{RID}, c'_{2,1}, V'_2))$. Since the random hash model is considered in the proof, $c'_{1,1}$ and $c'_{2,1}$ are uniformly distributed. Furthermore, since the underlying IBRS schemes for a domain are anonymous against full key exposure, the distributions of $c_{1,1} = \text{H}_1(\text{RID}, m,$ ***VComp***$(\pi_\omega, \text{RID}, c_{2,1}, V_2))$ and $c'_{1,1} = \text{H}_1(\text{RID}, m,$ ***VComp***$(\pi_\omega, \text{RID}, c'_{2,1}, V'_2))$ are (computationally) indistinguishable under full key exposure attacks. A similar reasoning can be applied to $c_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c_{1,1}, V_1))$ and $c'_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c'_{1,1}, V'_1))$, that is, $c_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c_{1,1}, V_1))$ and $c'_{2,1} = \text{H}_2(\text{RID}, m,$ ***VComp***$(\pi_\theta, \text{RID}, c'_{1,1}, V'_1))$ are (computationally) indistinguishable under full key exposure attacks. Thus, we have $(c_{1,1}, c_{2,1})$ and $(c'_{1,1}, c'_{2,1})$ being (computationally) indistinguishable under full key exposure attacks. Therefore, the extended IBRS scheme is anonymous against full key exposure. □

Theorem 6. The extended IBRS scheme is existentially unforgeable in the random oracle model.

Proof. The proof of the theorem mainly relies on a similar rewinding technique of [13] and [18][19][20]. We can simulate random hash functions, in a typical fashion, by selecting an element uniformly. Further, since the extended IBRS scheme follows a so-called commitment-challenge-response paradigm, and since we can control the simulation of the random hash functions, we can obviously simulate a signing oracle for the extended IBRS scheme by selecting a challenge as a hash output in advance. Assume that a forger generates a forged signature $\sigma = \{(c_{j,1},...,c_{j,t[j]},V_j) \mid 1 \le j \le k\}$. Let $h_j = \text{H}_j(\text{RID}, m,$ ***VComp***$(\pi_{j-1}, \text{RID}, c_{j-1,1},...,c_{j-1,t[j-1]},V_{j-1}))$. By using a rewinding technique, we can non-negligibly obtain another signature $\sigma' = \{(c'_{j,1},...,c'_{j,t[j]},V'_j) \mid 1 \le j \le k\}$ satisfying the following condition: Let $h'_j = \text{H}_j(\text{RID},$

m, ***VComp*** (π_{j-1}, RID, $c'_{j-1,1},...,c'_{j-1,t\,[j-1]}$, V'_{j-1})). For some $\beta \in \{1,\ldots,k\}$, and for $j = 1,...,k$ ($j \neq \beta$), $V_j = V'_j$, $h_j = h'_j$, and $V_\beta \neq V'_\beta$, $h_\beta \neq h'_\beta$. For $i = 1,...,t_{[\beta]}$ ($i \neq \gamma$), $c_{\beta,i} = c'_{\beta,i}$ and $c_{\beta,\gamma} \neq c'_{\beta,\gamma}$. Using a knowledge extractor with V_β, V'_β, $c_{\beta,\gamma}$, and $c'_{\beta,\gamma}$, an adversary can break an underlying IBRS scheme for single domains. This contradicts the unforgeability of the underlying IBRS schemes. Hence, the extended IBRS scheme is existentially unforgeable. □

2. A Concrete Instance for Multiple Domains

To further the understanding of our construction method for strongly separable IBRS schemes, let us now turn to an example using the IBRS schemes for a domain, which were suggested in the previous section. Let $\pi = (\pi_1, \pi_2)$, where π_1 and π_2 are public system parameters for the RSA-based IBRS scheme and the pairing-based IBRS scheme, respectively, i.e., $\pi_1 = (N, e, \mathrm{H}_{1,\mathrm{id}}, \mathrm{H}_1)$ and π_2=(**e**, G_1, G_2, G_T, q, P, P_{pub}, $\mathrm{H}_{2,\,\mathrm{id}}$, H_2).
For convenience, we denote the schemes by Σ_1 and Σ_2, respectively. Assume that a real signer has a signing key $sk_{2,\gamma} \in G_1$ for the second domain with π_2.

- **Sign.** Given π, a signing key $sk_{2,\gamma} \in G_1$, message m, and a ring RID = $\{(\pi_1, (\mathrm{ID}_{1,1},\ldots,\mathrm{ID}_{1,t'})), (\pi_2, (\mathrm{ID}_{2,1},\ldots,\mathrm{ID}_{2,t''})\}$, do the following:
  - ***Initialization***. Pick random $c''_i \in \{0,1\}^{L''}$ for $i = 1,...,t''$, ($i \neq \gamma$), and random $r_2 \in \mathrm{Z}_q^*$, and compute simulated commitment $B_2 \leftarrow \mathbf{e}(r_2 Q_{2,\gamma} + \sum_{i=1,\ldots,t''\,(i\neq\gamma)} c''_i Q_{2,i}, P_{pub})$ and challenge $w_1 \leftarrow \mathrm{H}_1(\mathrm{RID}, m, B_2)$, where $Q_{2,i} = \mathrm{H}_{2,\,\mathrm{id}}(\mathrm{ID}_{2,i})$.
  - ***Simulation***. For $i = 2,...,t'$, select $V_1 \in \mathrm{Z}_N^*$, $c'_i \in \mathrm{Z}_q^*$ at random, and compute $c'_1 = w_1 \oplus (\oplus_{i=2,\ldots,t'} c'_i)$, $B_1 \leftarrow V_1^e \cdot \Pi_{i=1,\ldots,t'} Q_{1,i}^{c'_i}$, and $w_2 \leftarrow \mathrm{H}_2(\mathrm{RID}, m, B_1)$, where $Q_{1,i} = \mathrm{H}_{1,\,\mathrm{id}}(\mathrm{ID}_{1,i})$.
  - ***Real Proof***. Compute $c''_\gamma = w_2 \oplus (\oplus_{i=2,\ldots,t''\,(i\neq\gamma)} c''_i)$ and $V_2 = (r_2 - c''_\gamma)\, sk_{2,\gamma}$.

Output signature $\sigma = \{(c'_1,...,c'_{t'}, V_1), (c''_1,...,c''_{t''}, V_2)\}$.

- **Vrfy**. Given π, a message m, and $\sigma = \{(c'_1,...,c'_{t'}, V_1), (c''_1,...,c''_{t''}, V_2)\}$, compute $B_1' \leftarrow V_1^e \cdot \Pi_{i=1,\ldots t'} Q_{1,i}^{c'_i}$ and $B_2' \leftarrow \mathbf{e}(V_2, P) \cdot \mathbf{e}(\sum_{i=1,\ldots t''} c''_i Q_{2,i}, P_{pub})$. Check if $\oplus_{i=1,\ldots,t''} c''_i = \mathrm{H}_2(\mathrm{RID}, m, B_1')$ and $\oplus_{i=1,\ldots,t'} c'_i = \mathrm{H}_1(\mathrm{RID}, m, B_2')$. If the equality holds, then output 1; otherwise, output 0.

Similarly, a real signer with the signing key $sk_{1,\eta}$ for the first domain π_1 is able to generate a ring signature of which the ring consists of ring members chosen from the two different domains.

5. Performance Comparison

In this section, we present a performance comparison between our schemes and some of the best-known IBRS schemes with respect to the size of signatures and computational costs. For convenience we denote by IBRS-1 and IBRS-2 our RSA-based IBRS scheme and our pairing-based IBRS scheme, respectively.

In this analysis, we define some notations: n is the number of all ring members in a ring of a given signature. *Dnum* is the number of all different domains in a ring of a given signature. L_{hash} is the bit-length of a given hash function to generate parameters c_j. *Exp* is a modulo exponentiation under a RSA modulus. S is a scalar multiplication on G_1 , and P is a pairing

operation. L_N and L_{G1} are the bit-length of an RSA modulus N and the shortest group G_1 defined for a pairing map, respectively.

First, we compare our IBRS schemes for single domains with the IBRS schemes by [4] and [5] [See **Table 1**.].

Table 1. Performance Comparison.

	Sig-Length (bit)	Computational Costs		Param.	Security
		Sign	Vrify		
[5]	$(1+n)\cdot L_N$	$2n\cdot Exp$	$(n+1)\cdot Exp$	RSA	RSA Problem
Our IBRS-1	$n\cdot L_{hash}+L_N$	$(n+2)\cdot Exp$	$(n+1)\cdot Exp$	RSA	RSA Problem
[4]	$(1+n)\cdot L_{G1}$	$(n+1)\cdot S$	$n\cdot S+2\cdot P$	Pairing	CDH Problem
Our IBRS-2	$n\cdot L_{hash}+L_{G1}$	$(n+1)\cdot S+1\cdot P$	$n\cdot S+2\cdot P$	Pairing	CDH Problem

Currently, $L_{hash} = 160$ and $L_N = 1024$ are considered practically secure. Meanwhile, to achieve the same security level as an 1024-bit RSA system, the bit-length of group G_1 for a pairing map must be 171 bits. Note that this assumption can be obtained by using MNT curves [21]. Let $L_{G1} = 171$. As summarized in Table 1, the signature length of our IBRS-1 is $n\cdot L_{hash} + L_N$ and that of the RSA-based IBRS scheme [5] is $(n+1)\cdot L_N$. $(n\cdot L_{hash}+L_N)/(n+1) \cdot L_N$ becomes asymptotically close to $w = L_{hash}/L_N$, as n, the size of a ring, increases. Thus, the ratio $w = 160/1024 = 0.156$ for $L_{hash} = 160$ and $L_N = 1024$. In this case, our IBRS-1 is 84% more efficient, compared to the scheme of [5]. Using a similar analysis, we can show that our IBRS-2 is 7% more efficient, compared to the pairing-based IBRS scheme [4]. As can be noted in Table 1, our IBRS-2 is comparable to the scheme of [4], and our IBRS-1outperforms the scheme of [5] in terms of signing and verifying costs.

Next, we compare our generic IBRS scheme for multiple domains with the separable IBRS scheme of [13]. Let |OURS| and |AHR| denote the signature size of [13] and that of our scheme, respectively. We can summarize the signature sizes of the two schemes as follows:

$$|\text{OURS}| = \Sigma_{i=1,\ldots,Dnum}\,(L_{V_i} + \Sigma_{j=1,\ldots,n_i} L_{hash_j}),$$
$$|\text{AHR}| = \Sigma_{i=1,\ldots,Dnum}\,\Sigma_{j=1,\ldots,n_i}(L_{V_j} + L_{hash_j}),$$

where L_{V_i} denotes the size of each variable V_j in signature $\{(c_{j,1},\ldots,c_{j,t[jj]}, V_j) \mid 1 \le j \le k\}$. It is easy to see that $|\text{OURS}| \le |\text{AHR}|$ because $|\text{OURS}| - |\text{AHR}| = \Sigma_{i=1,\ldots,Dnum} L_{V_i} - \Sigma_{i=1,\ldots,Dnum}\,\Sigma_{j=1,\ldots,n_i} L_{V_j} \le 0$ for positive integers L_{V_k}. The equality only holds when $n_i = 1$ for all i; that is, only one signer is chosen from each domain.

5. Conclusion

We have proposed generic methods to construct IBRS schemes with varying levels of separability. We first presented a method for constructing an IBRS for a single domain. We then presented a generic method for constructing IBRS schemes for multiple domains by extending the IBRS schemes for a single domain. We showed that our method results in short signatures. We also demonstrated that the schemes presented are secure in the random oracle model. An interesting open problem would be to construct a secure IBRS scheme for multiple domains without a random oracle.

References

[1] L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology - ASIACRYPT'01*, LNCS 2248, 2001, pp. 552-565. Article(CrossRef Link)

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology - CRYPTO'84*, LNCS 196, 1985, pp. 47-53. Article(CrossRef Link)

[3] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in *Advances in Cryptology - EUROCRYPT'04*, 2009, LNCS 3027, pp. 268-286. Article(CrossRef Link)

[4] S. S.M. Chow, S.M. Yiu, and L. C.K. Hui, "Efficient identity based ring signature," in *ACNS'05*, 2005, LNCS 3531, pp. 499-512. Article(CrossRef Link)

[5] J. Herranz, "Identity-based ring signatures from RSA," in *Theoretical Computer Science*, 2007, vol. 389 (1-2), pp. 100-117. Article (CrossRef Link)

[6] M. Abe, M. Ohkubo, and K. Suzuki, "1-Out-of-n signatures from a variety of keys," in *Advances in Cryptology - ASIACRYPT'02*, LNCS 2501, 2002, pp. 415-432. Article(CrossRef Link)

[7] Guillou and J.J. Quisquater, "A Paradoxical" Identity-Based Signature Scheme Resulting from Zero-knowledge," in *Advances in Cryptology - CRYPTO'88*, 1990, LNCS 403, pp. 216-231. Article(CrossRef Link)

[8] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman Groups," in *Public Key Cryptography – PKC'03*, LNCS 2139, 2003, pp. 18-30. Article(CrossRef Link)

[9] F. Hess, "Efficient Identity Based Signature Schemes on Pairings," in *Selected Areas in Cryptography – SAC'02*, LNCS 2595, 2003, pp. 310-324. Article(CrossRef Link)

[10] J. Herranz, "Formal Proof of Security of Zhang and Kim's ID-Based Ring Signature Scheme," International Workshop on Security in Information Systems, in *WOSIS'04*, 2004, pp. 63-72. Article(CrossRef Link)

[11] F. Zhang and K. Kim, "ID-based Blind Signature and Ring Signature from Pairings," in *Advances in Cryptology - ASIACRYPT'02*, LNCS 2501, 2002, pp. 533-547. Article(CrossRef Link)

[12] A. Bender, J. Katz, and R. Morselli, "Ring Signatures: Stronger Definitions, and Constructions without Random Oracles," in *Proceedings of TCC'06*, LNCS 3876, 2006, vol. 3876, pp. 60-79. Article(CrossRef Link)

[13] B. Adida, S. Hohenberger, and R. L. Rivest, "Separable Identity-Based Signature: Theoretical Foundation For Fighting Phishing Attacks," Computer Science and Artificial Intelligence Laboratory; MIT. Article(CrossRef Link)

[14] K. Lee, J. Y. Hwang, and D. H. Lee, "Non-Interactive Identity-Based DNF Signature Scheme and Its Extensions," in *Bulletin of the Korean Mathematical Society*, 2009, vol. 46, no. 4, pp. 743-769. Article(CrossRef Link)

[15] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols," in *Advances in Cryptology - CRYPTO'94*, 2004, LNCS 839, pp. 174-187. Article(CrossRef Link)

[16] J. Camenisch and M. Michels, "Separability and Efficiency for Generic Group Signature Schemes," in *Advances in Cryptology - CRYPTO'99*, 1999, LNCS 1666, pp. 413-430. Article(CrossRef Link)

[17] J. E. Nymann, "On the Probability that Positive Integers are Relatively Prime," J. Number Th., vol. 4, 1972, pp. 469-473. Article (CrossRef Link)

[18] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification

and Signature Problems," in *Advances in Cryptology - CRYPTO'86*, 1987, LNCS 263, pp. 186-199. Article(CrossRef Link)
[19] K. Ohta and T. Okamoto, "On Concrete Security Treatment of Signatures Devised from Identification," in *Advances in Cryptology - CRYPTO'98*, LNCS 1462, 1998, pp. 354-369. Article(CrossRef Link)
[20] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," in *J. of Cryptology*, vol. 13, 2000, pp. 361-396. Article (CrossRef Link)
[21] X. Boyen, "A Tapestry of Identity-Based Encryption: Practical Frameworks Compared," in *Int. J. Applied Cryptography*, Vol. 1, No. 1, 2008, Inderscience, pp. 3-21. Article(CrossRef Link)

JuHee Ki received the B.S. degree in Mathematics from University of Seoul and the M.S. degree in Information Security from Korea University, Korea in 2001 and 2003, respectively. Since 2003, she has been a researcher of KEIT (Korea Evaluation Institute of Industrial Technology), Korea. Her main research interests include cryptography, broadcast encryption, digital signatures, Identity-based cryptography, attribute-based cryptography, and their applications. Also, she is interested in privacy-enhancing cryptography.

Jung Yeon Hwang received the B.Sc. degree in Mathematics from Korea University, the M.S. and Ph.D. degrees in information security from Korea University, Korea on 1999, 2003, and 2006 respectively. He has been a post-doctoral researcher of Korea University from 2006 to 2009. Since 2009, he has been a senior member of engineering staff of Electronics and Telecommunications Research Institute (ETRI), Korea. Dr. Hwang's research interests include cryptography, broadcast encryption, digital signatures, Identity-based cryptography, attribute-based cryptography, and their applications. Also, he is interested in privacy-enhancing techniques.

Dong Hoon Lee received the B.S. degree from the Department of Economics at Korea University, Seoul, in 1985, and the M.S. and Ph.D. degrees in computer science from the University of Oklahoma, Norman, in 1988 and 1992, respectively. Currently he is a professor and the vice director of the Graduate School of Information Security at Korea University. His main research interests include the design and analysis of cryptographic protocols in key agreement, encryption, signature, embedded device security, and privacy-enhancing technology.