Concise Papers

Ring Signature with Weak Linkability and Its Applications

Ik Rae Jeong, Jeong Ok Kwon, and Dong Hoon Lee, *Member, IEEE*

Abstract—We suggest a linkable ring signature scheme providing *strong anonymity* and *weak linkability*. We show that our linkable ring signature scheme can be used to construct a *selectively* linkable ring signature scheme, an efficient *convertible (verifiable)* ring signature scheme, and an efficient *deductible* ring signature scheme.

Index Terms—Ring signature, linkability, selectivity, convertibility, deductibility.

1 Introduction

The 1-out-of-n group signature without the group manager, called "ring signature," was presented by Chen and Pedersen [3] and by Rivest et al. [9]. Usually, the group signature requires the group manager, but the ring signature needs no group manager. A signer himself constructs an arbitrary group (or a "ring") of parties and, then, signs on behalf of the ring. The ring signature provides anonymity of an actual signer as in the group signature.

We review some security requirements of ring signatures. Ring signatures must have the following properties [3], [9]:

- Unforgeability. Only a party in a ring can make a ring signature on behalf of the ring.
- Strong anonymity. Any party cannot know the actual signer of a ring signature, even if all of the private keys of the parties of the ring are known.
- Exculpability. An actual signer can deny that he has made a ring signature, even if his private key is known. Note that if a ring signature scheme provides anonymity, the signature scheme also provides exculpability.

Liu et al. suggested a notion of *linkable* ring signature and a linkable ring signature scheme [6].

A linkable ring signature provides anonymity of an actual signer, but the generated signatures are linkable. That is, any party can know whether or not the ring signatures are made by the same signer, although the party cannot know the identity of the actual signer.

Liu et al. remarked that their linkable ring signature scheme does not provide *strong* anonymity and designing a linkable ring signature scheme with strong anonymity is an open problem. Following the approach in [6], several linkable ring signature schemes have been suggested in [11], [10], [1], [2], [5], [12]. However, all of the previous schemes still do not provide strong anonymity. That is, the previous linkable ring signature schemes provide *weak anonymity* and *strong linkability*.

In some applications such as "whistle blowing," we cannot use the linkable ring signature schemes that have weak anonymity and strong linkability. A whistle blower in an organization wants to give some information to the authority or to the public. In this case, the whistle blower definitely does not want to reveal his identity even if all of the other parties in the organization cooperate to find the identity of the whistle blower. So, the linkable ring signature schemes that have weak anonymity and strong linkability are not suitable for whistle blowing, since the identity of a whistle blower is easily recovered through the cooperation of the other parties in the organization. Suppose that the whistle blower wants to give some additional information and say that he or she is the same entity with the previous whistle blower without revealing his identity. This linkability is useful, because if the previous information is reliable, then the additional information is likely to be reliable. The "selectively" linkable ring signature scheme (defined below) can be used in whistle blowing.

In our work, we construct a ring signature scheme providing *strong anonymity* and *weak linkability*. Our linkable ring signature scheme can be used to construct the following ring signature scheme:

1. The *selectively* linkable ring signature scheme. In a selectively linkable ring signature scheme, a signer can generate the ring signatures without linkability. However, the signer can later choose some of the ring signatures and convert the signatures into linkable ring signatures. Our scheme is the first ring signature scheme with selective linkability.
2. The efficient *convertible (verifiable)* ring signature scheme. In a convertible ring signature scheme, a signer can prove that he or she is the actual signer of a ring signature. In our scheme, a signer stores only *one* random number, whereas in the previous schemes in [9] and [7] the number of random numbers stored by a signer linearly increases if the number of signatures increases.
3. The efficient *deductible* ring signature scheme. In a deductible ring signature scheme, the actual signer can prove that the other party in a ring is not the signer of a ring signature. Of course, the actual signer cannot prove that he or she is not the signer of a ring signature. In our scheme, a signer stores only *one* random number, whereas in the previous schemes in [9] the number of random numbers stored by a signer linearly increases if the number of signatures increases.

2 Anonymity versus Linkability in Linkable Ring Signature

In [6], Liu et al. suggested a *linkable* ring signature scheme, which has the following properties:

- Unforgeability. Only a party in a ring can make a ring signature on behalf of the ring.
- Weak anonymity. Any party cannot know the actual signer of a ring signature, only if all of the parties of the ring do not reveal their identities.
- Linkability. Any party can know whether or not the ring signatures are made by the same signer, although the party cannot know the identity of the actual signer.
- Culpability. An actual signer cannot deny that he has made a ring signature, if his private key is known.

With respect to the linkability, Liu et al. defined the *strong linkability* as follows [6]:

- *The authors are with the Graduate School of Information Security CIST, Korea University 1, 5-Ka, Anam-dong Sungbuk-ku, Seoul,136-701 Korea. E-mail: {irjeong, pitapat, donghlee}@korea.ac.kr.*

Manuscript received 16 May 2007; revised 4 Nov. 2007; accepted 21 Dec. 2007; published online 11 Jan. 2008.
For information on obtaining reprints of this article, please send e-mail to: tkde@computer.org, and reference IEEECS Log Number TKDE-2007-05-0221.
Digital Object Identifier no. 10.1109/TKDE.2008.19.

1041-4347/08/$25.00 © 2008 IEEE Published by the IEEE Computer Society

1. For a ring, a signer in the ring cannot make two ring signatures that are not linkable.
2. A signer in a ring cannot make a ring signature that is linkable to the ring signatures made by the other signer in the ring.

It has been observed that a scheme providing culpability does not provide strong anonymity and exculpability. That is, if all of the other parties of a ring without an actual signer collaborate, they can prove that a ring signature was made by the actual signer. Thus, all of the linkable ring signature schemes in [6], [11], [10], [1], [2], [5], and [12] provide only *weak anonymity*.

In the following theorem, we show that it is impossible to make a ring signature scheme that provides both strong anonymity and strong linkability.

Theorem 1. *It is impossible to make a ring signature scheme that provides both strong anonymity and strong linkability.*

Proof of Theorem 1. Suppose that we have a ring signature σ, which is made by a ring signature scheme providing both strong anonymity and strong linkability. Let $\mathcal{A}$ be an adversary attacking strong anonymity with all of the private keys of the parties in the ring of σ and trying to recover the identity of the actual signer of σ. Let $(P_1, \ldots, P_n)$ be the parties in the ring of σ. For $1 \le i \le n$, $\mathcal{A}$ makes a ring signature τ_i with the private key of P_i and checks whether or not τ_i and σ are linkable. If τ_i and σ are linkable, $\mathcal{A}$ can know that P_i is the actual signer of σ. Note that this attack strategy of $\mathcal{A}$ is always successful. Because the ring signature scheme provides strong linkability, σ should be linkable to one of ring signatures $(\tau_1, \ldots, \tau_n)$. Therefore, if a ring signature scheme provides strong linkability, the ring signature scheme does not provide strong anonymity. □

To make a ring signature scheme providing strong anonymity and linkability, we weaken the definition of linkability. We suggest the *weak linkability* that has the following properties:

1. For a ring, a signer in the ring can make ring signatures that are linkable. A signer in the ring can also make ring signatures that are not linkable.
2. A signer in a ring cannot make a ring signature that is linkable to the ring signatures made by the other signer in the ring.

3 Linkable Ring Signature with Weak Anonymity and Strong Linkability

The ring signature schemes suggested in [11], [10], [1], [2], and [5] follow the construction paradigm in [6].

A ring signature in [6] contains a "link tag," $\tilde{y} = H_2(\mathcal{L})^{x_\pi}$, to provide linkability, where $\mathcal{L}$ is a list of the public keys of a ring, H_2 is a hash function, and x_π is a private key of a signer. Note that the link tag $\tilde{y}$ uses only a private key and the public information without any random number. The culpability and weak anonymity are from the following fact: The link tag is "reconstructible" if a private key and the public information are given. The ring signature schemes in [11], [10], [1], [2], and [5] also use a reconstructible tag, so the ring signature schemes in [6], [11], [10], [1], [2], and [5] provide culpability and weak anonymity.

4 Our Linkable Ring Signature Scheme with Strong Anonymity and Weak Linkability

The basic idea of our scheme is to make a link tag of a ring signature using random numbers such that the link tag is not reconstructible with a private key and the public information.

Let $\mathbb{G} = \langle g \rangle$ be a group of prime order q such that the underlying discrete logarithm problem (DLP) is intractable. Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$ be a hash function. Each party P_i has a pair of private/public keys $(x_i, y_i = g^{x_i})$.

Ring signature generation. Assume that a ring is $\mathcal{R} = \{P_1, \ldots, P_n\}$ and $P_\pi \in \mathcal{R}$ wants to sign message m on behalf of ring $\mathcal{R}$. The following algorithm generates a linkable ring signature:

1. Pick randomly D_0 from $\mathbb{G}$ and a from $\mathbb{Z}_q$. Compute $D_1 = D_0^a$. The random numbers should be selected uniformly and independently.
2. Pick randomly u, v from $\mathbb{Z}_q$, and compute $R_\pi = g^u$ and $R_A = D_0^v$. The random numbers should be selected uniformly and independently.
3. For i $(1 \le i \le n,\ i \ne \pi)$, pick c_i, s_i from $\mathbb{Z}_q$ and compute $R_i = g^{s_i} y_i^{c_i}$.
4. Compute $c = H(D_0, D_1, m, R_1, \ldots, R_n, R_A)$.
5. Compute c_π such that $c = c_1 + \cdots + c_\pi + \cdots + c_n \bmod q$, $s_\pi = u - x_\pi c_\pi \bmod q$, and $s_A = v - ac \bmod q$.

The signature is $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$.

Ring signature verification. To check a signature $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$ on message m, the verifier checks

$$c \overset{?}{=} H(D_0, D_1, m, g^{s_1} y_1^{c_1}, \ldots, g^{s_n} y_n^{c_n}, D_0^{s_A} D_1^c),$$

where $c = c_1 + \cdots + c_n \bmod q$. If the verification is successful, accept. Otherwise, reject.

4.1 Security Analysis

Our ring signature scheme provides unforgeability, strong anonymity, weak linkability, and exculpability.

Unforgeability. Without knowing at least one private key of the parties in a ring, any party cannot make a ring signature on behalf of the ring.

Theorem 2. *Our ring signature scheme provides unforgeability.*

Proof of Theorem 2. If an algorithm $\mathcal{A}$ can make a ring signature, we can make an extractor E using $\mathcal{A}$ in the random oracle model [8]. Assume that $\mathcal{A}$ outputs $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$. Then, E can get another signature $\sigma'(m) = (D_0, D_1, c_1', \ldots, c_n', s_1', \ldots, s_n', s_A')$ using the standard "rewinding" technique [8].

In the random oracle model, E simulates the hash oracle H and answers for the hash queries. E outputs two different c and $c'(\ne c)$ for the same hash query $(D_0, D_1, m, R_1, \ldots, R_n, R_A)$, where $c = c_1 + \cdots + c_n \bmod q$ and $c' = c_1' + \cdots + c_n' \bmod q$. Then, there should be $c_i \ne c_i'$, where $i \in [1, n]$. From (c_i, s_i) and (c_i', s_i'), E can calculate the private key $x_i = \frac{s_i - s_i'}{c_i' - c_i}$. So, if an algorithm generates valid ring signatures, the algorithm knows at least one private key. □

Strong anonymity and exculpability. Even if a party knows all of the private keys of the parties and the random number $a = \log_{D_0} D_1$, the party cannot know the identity of the actual signer of a ring signature.

Theorem 3. *Our ring signature scheme provides strong anonymity.*

Proof of Theorem 3. Let a ring signature for message m be $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$. It is obvious that $s_i = \log_g R_i - x_i c_i \bmod q$ for $1 \le i \le n$. So, even an algorithm having an infinite power cannot know which party in a ring has made $\sigma(m)$. □

Weak linkability. If P_π uses the same (D_0, a) in two signatures, the link tags (D_0, D_1) are the same. So, the two signatures are linkable. If P_π uses (D_0, a) and (D_0', a') in two signatures, the link tags $(D_0, D_1(= D_0^a))$ and $(D_0', D_1'(= D_0'^{a'}))$ are different. So, the signatures are not linkable.

TABLE 1
Comparison between Ring Signature Schemes

	[9]	[6]	Our scheme
Num. of terms in a signature	$n+1$	$n+2$	$2n+3$
Num. of exp.	sign:1 ver.:n	sign:$4n-1$ ver.:$4n$	sign:$2n+1$ ver.:$2n+2$
Anonymity	strong	weak	strong
Linkability	no	strong	weak

Assume that P_π has made

$$\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A).$$

P_i ($\neq P_\pi$) in a ring can make

$$\sigma'(m') = (D_0, D'_1, c'_1, \ldots, c'_n, s'_1, \ldots, s'_n, s'_A)$$

by selecting a' and calculating $D'_1 = D_0^{a'}$. P_i ($\neq P_\pi$) in a ring can also make $\sigma'(m') = (D'_0, D_1, c'_1, \ldots, c'_n, s'_1, \ldots, s'_n, s'_A)$ by selecting a' and calculating $D'_0 = D_1^{(a')^{-1}}$. However, any other party except P_π cannot make a ring signature

$$\sigma(m') = (D_0, D_1, c'_1, \ldots, c'_n, s'_1, \ldots, s'_n, s'_A)$$

without knowing a.

Theorem 4. *Our ring signature scheme provides weak linkability.*

Proof of Theorem 4. Let a ring signature for message m be $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$. If an algorithm $\mathcal{A}$ can make a ring signature for message m' with the same (D_0, D_1), we can make an extractor E using $\mathcal{A}$ in the random oracle model. Assume that $\mathcal{A}$ outputs

$$\sigma'(m') = (D_0, D_1, c'_1, \ldots, c'_n, s'_1, \ldots, s'_n, s'_A).$$

Then, E can get another signature

$$\sigma''(m') = (D_0, D_1, c''_1, \ldots, c''_n, s''_1, \ldots, s''_n, s''_A)$$

using the rewinding technique.

In the random oracle model, E simulates the hash oracle H and answers for the hash queries. E outputs two different c' and $c''(\neq c')$ for the same hash query $(D_0, D_1, m', R'_1, \ldots, R'_n, R'_A)$. From (c', s'_A) and (c'', s''_A), E can calculate the discrete logarithm $a = \log_{D_0} D_1 = \frac{s'_A - s''_A}{c'' - c'}$. So, if an algorithm can generate linkable ring signatures to any given ring signature, we can solve the DLP using the algorithm. Note that DLP is one of the most basic and hard problem in cryptography. □

4.2 Efficiency

Let n be the number of parties in a ring. We compare the ring signature schemes in [9] and [6] with our scheme in Table 1.

5 The Applications of Our Linkable Ring Signature Scheme

The selectively linkable ring signature scheme. A signer may not want the linkability at the time when he makes the ring signatures. However, the signer may later want to prove that the ring signatures are made by the same signer. This selective linkability is possible as follows: P_π makes the ring signatures

$$\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A) \text{ and}$$
$$\sigma'(m) = (D'_0, D'_1, c'_1, \ldots, c'_n, s'_1, \ldots, s'_n, s'_A),$$

where $D_1 = D_0^a$ and $D'_1 = D'^a_0$. Then, $\sigma(m)$ and $\sigma'(m)$ are not linkable, since anyone cannot decide the equality of discrete logarithms $\log_{D_0}(D_1) \overset{?}{=} \log_{D'_0}(D'_1)$. P_π can later prove that $\sigma(m)$ and $\sigma'(m)$ are made by the same signer by giving a proof $\Gamma = Proof[(a) : D_1 = D_0^a \wedge D'_1 = D'^a_0]$, which proves the knowledge of the discrete logarithms and $\log_{D_0}(D_1) = \log_{D'_0}(D'_1)$. Note that Γ can be efficiently made using the noninteractive proof system in [4].

TABLE 2
Comparison between Convertible Ring Signature Schemes

	[9]	Our scheme
Num. of terms in a signature	$n+1$	$2n+3$
Num. of exp.	sign:1 ver.:n	sign:$2n+1$ ver.:$2n+2$
Number of secrets	$N_s(n-1)$	1

n: the number of parties in a ring
N_s: the number of issued signatures

The convertible ring signature scheme. An actual signer can later prove that he has made the ring signatures. If P_π wants to prove that P_π has made a ring signature

$$\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A),$$

P_π gives to a verifier $\Delta = Proof[(x_\pi, a) : y_\pi = g^{x_\pi} \wedge D_1 = D_0^a]$, which proves the knowledge of the discrete logarithms. Then, the verifier checks Δ. If the verification is successful, the verifier accepts that P_π has made the ring signature.

The deductible ring signature scheme. Assume that P_π has made a ring signature $\sigma(m) = (D_0, D_1, c_1, \ldots, c_n, s_1, \ldots, s_n, s_A)$ for a ring $\mathcal{R} = \{P_1, \ldots, P_n\}$. P_π can later prove that the real signer is not $P_k (1 \leq k \leq n, k \neq \pi)$ as follows: P_π makes a ring signature $\sigma'(m) = (D_0, D_1, c'_1, \ldots, c'_{n-1}, s'_1, \ldots, s'_{n-1}, s'_A)$ for a ring $\mathcal{R}' = \mathcal{R} - \{P_k\}$. If $\sigma'(m)$ is valid, the verifier assures that the real signer is not P_k from the following facts:

1. Because a used in the two ring signatures, $\sigma(m)$ and $\sigma'(m)$, is the same, the verifier assures that $\sigma(m)$ and $\sigma'(m)$ are made by the same signer.
2. From unforgeability, the verifier assures that the real signer of $\sigma(m)$ and $\sigma'(m)$ must be one in $\mathcal{R} \cap \mathcal{R}' = \mathcal{R}'$.

Efficiency. The ring signature scheme with convertibility and deductibility in [9] requires that a signer should use fresh random seeds to make a ring signature. The random seeds are used for convertibility and deductibility. So, a signer has to keep $N_s(n-1)$ random numbers for convertibility and deductibility, if the signer has made N_s ring signatures and n is the number of parties in a ring. Thus, the scheme is not practical for convertible or deductible ring signatures. In our scheme with selective linkability, convertibility, and deductibility, a signer keeps only one random number a. The comparison between the convertible ring signature schemes is given in Table 2.

The comparison between deductible ring signature schemes is given in Table 3.

6 Conclusion

We have shown that the linkable ring signature schemes in [6], [11], [10], [1], [2], and [5] do not provide strong anonymity. We

TABLE 3
Comparison between Deductible Ring Signature Schemes

	[9]	Our scheme
Num. of terms in a signature	$n+1$	$2n+3$
Num. of exp.	sign:1 ver.:n	sign:$2n+1$ ver.:$2n+2$
Number of secrets	$N_s(n-1)$	1

n: the number of parties in a ring
N_s: the number of issued signatures

have then suggested a linkable ring signature scheme providing strong anonymity and weak linkability.

Our linkable ring signature scheme can be used to construct a selectively linkable ring signature scheme, a convertible (verifiable) ring signature scheme, and an efficient ring signature scheme.

Acknowledgments

The authors would like to thank the anonymous reviewers for their many useful comments and suggestions. This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2008-(C1090-0801-0025)).

References

[1] M.H. Au, S.S.M. Chow, W. Susilo, and P.P. Tsang, "Short Linkable Ring Signatures Revisited," *Proc. Third European PKI Workshop: Theory and Practice (EuroPKI '06),* pp. 101-115, 2006.

[2] M.H. Au, J.K. Liu, W. Susilo, and T.H. Yuen, "Constant-Size ID-Based Linkable and Revocable-Iff-Linked Ring Signature," *Proc. Int'l Conf. Cryptology in India (INDOCRYPT '06),* pp. 364-378, 2006.

[3] L. Chen and T.P. Pedersen, "New Group Signature Schemes," *Proc. Workshop Theory and Application of Cryptographic Techniques (EUROCRYPT '94),* pp. 171-181, 1994.

[4] J. Camenisch and M. Stadler, "Efficient Group Signature Scheme for Large Groups," *Proc. 17th Ann. Int'l Cryptology Conf. (CRYPTO '97),* pp. 410-424, 1997.

[5] J.K. Liu and D.S. Wong, "Enhanced Security Models and a Generic Construction Approach for Linkable Ring Signature," *Int'l J. Foundations of Computer Science,* vol. 17, no. 6, pp. 1403-1422, Dec. 2006.

[6] J.K. Liu, V.K. Wei, and D.S. Wong, "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups," *Proc. Ninth Australasian Conf. Information Security and Privacy (ACISP '04),* pp. 325-335, 2004.

[7] J. Lv and X. Wang, "Verifiable Ring Signature," *Proc. Ninth Int'l Conf. Distributed Multimedia Systems (DMS '03),* pp. 663-667, 2003.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," *J. Cryptology,* vol. 13, no. 3, pp. 361-396, 2000.

[9] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," *Proc. Advances in Cryptology, Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT '01),* pp. 552-565, 2001.

[10] P.P. Tsang and V.K. Wei, "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation," *Proc. First Information Security Practice and Experience Conf. (ISPEC '05),* pp. 48-60, 2005.

[11] P.P. Tsang, V.K. Wei, T.K. Chan, M.H. Au, J.K. Liu, and D.S. Wong, "Separable Linkable Threshold Ring Signatures," *Proc. Int'l Conf. Cryptology in India (INDOCRYPT '04),* pp. 384-398, 2004.

[12] D. Zheng, V.K. Wei, and K.F. Chen, "GDH Group-Based Signature Scheme with Linkability," *IEE Proc. Comm.,* vol. 153, no. 5, pp. 639-644, Oct. 2006.

▷ **For more information on this or any other computing topic, please visit our Digital Library at** www.computer.org/publications/dlib.