ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings

Amit K Awasthi[1] and Sunder Lal[2]

[1] Department of Applied Science
Hindustan College of Science and Technology
Farah, Mathura -281122, INDIA
awasthi_hcst@yahoo.com
[2] Department of Mathematics
I. B. S. Khandari, Agra - INDIA

Abstract. In 2001, Rivest et al. firstly introduced the concept of ring signatures. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. The first scheme proposed by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. The first ring signature scheme based on DLP was proposed by Abe, Ohkubo, and Suzuki. Their scheme is also based on the general certificate-based public key setting too. In 2002, Zhang and Kim proposed a new ID-based ring signature scheme using pairings. Later Lin and Wu proposed a more efficient ID-based ring signature scheme. Both these schemes have some inconsistency in computational aspect.
In this paper we propose a new ID-based ring signature scheme and a proxy ring signature scheme. Both the schemes are more efficient than existing one. These schemes also take care of the inconsistencies in above two schemes.
Keywords: Cryptography, Digital Signature, Ring Signature, Bilinear pairings, ID-based.

1 Introduction

The concept of ring signature was introduced by Rivest, Shamir and Tauman in [13]. The ring signature allows a user from a set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed. The ring signature may be considered to be a simplified group signature which consists of only users without the managers. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but doesn't know exactly who the signer is. There is no way to revoke the anonymity of the signer.

Unlike the group signature schemes the ring signature scheme requires neither a group manager, nor a setup procedure, nor the action of non-signing members. For signing any message m, the signer may choose random set of other possible signers including himself, to produce a valid ring signature. This signature does not reveal the identity of the signer but it may be verified with this signature that the signer belong to the possible signers set. There is no revocation manager. This allows unconditional anonymity of signer.

Ring Signature with Proxy Signatures: The proxy signature scheme was introduced by Mambo et al. in 1996. These allow a proxy signer to sign on behalf of an original signer. After Mambo et al. many proxy signature schemes have been proposed [9, 11, 15]. Proxy signature may be combined with other special signatures to obtain new type of the proxy signatures. Various schemes like multi-proxy signature scheme [8], threshold proxy signature scheme, proxy blind signature scheme [10] etc. have been proposed.

Suppose an original signer delegates its signing capability to a number of proxy signers, such that any proxy signer may produce a valid proxy signature for some message m. To achieve anonymity of these proxy signers we may use ring signatures. We, therefore, combine the idea of proxy signature with ring signature and get a new type of signature - *proxy ring signature*.

In 1984, Shamir [14] introduced ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting. Recently, many bilinear pairings based ID-based signature schemes were developed. [1–7, 16, 17]

In this paper we propose a new ID-based ring signature scheme and also an ID-based proxy ring signature scheme. Both schemes are more efficient than existing schemes.

2 Overview of Ring Signatures

In this section we follow formalization proposed by Rivest et al. [13]

Definition 1. *Assume that each user has a secret key S_i and its corresponding public key P_i. Let $< P_r >$ denotes the set of possible signer where r is number of users listed in the set. Then ring signature scheme consists of the following algorithms –*

- *Ring Sign- A probabilistic algorithm which takes a message m, secret key S_k of signer, and the possible signers set $< P_r >$ as input and produces a ring signature σ for the message m*
- *Ring Verify- A deterministic algorithm which takes a message m, the possible signers set $< P_r >$ and the ring signature σ as input and returns either* `TRUE` *or* `FALSE`.

2.1 Properties

A ring signature must satisfy the usual correctness and unforgeability property. A fairly generated ring signature must be accepted as valid with higher probability; and it must be infeasible for any other user to generate, except a very little probability ϵ, a valid ring signature with the ring he does not belong to.

Signature must be anonymous, so that no verifier should be able to guess the actual signer's identity with probability greater than $\frac{1}{r} + \epsilon$, where r is ring size and ϵ is however small.

Since the possible signer set is randomly chosen and is not predetermined, it should be a part of signature.

2.2 Combining Function

The concept of *Ring signature* is derived from an abstract concept called *Combining Function.*

Definition 2. *A combining function $C_{k,v}(y_1, y_2, ..., y_n)$ takes as input a key k, an initialization value (also refereed as glue value) v, and an arbitrary values $y_1, y_2, ..., y_n \in \{0,1\}^b$. It produces $z \in \{0,1\}^b$, such that for any fixed values k, v, any index s and fixed value of $\{y_i\}_{i \neq s}, C_{k,v}$ is a permutation over $\{0,1\}^b$, when seen as a function of y_s. This permutation is efficiently computable as well as its inverse.*

2.3 Rivest et al.'s Ring signature scheme

Ring signature generation: Given a message m to be signed, signer's secret key S_k, and the possible signers' public keys sequence $P_1, P_2, ..., P_r$ of all ring members, the signer computes the ring signature as follows.

1. **Choose a key** : The signer computes, using a publicly known hash function h
$$k = h(m, P_1, P_2, ..., P_r)$$
2. **Pick a random glue value** : The signer picks an initialization value $v \in_R \{0,1\}^b$
3. **Pick random x_i's** : The signer picks an random x_i for all other ring members uniformly and independently from $\{0,1\}^b$, and computes $y_i = g_i(x_i)$.
4. **Formation of ring** : The signer solves the ring equation for y_k:
$$C_{k,v}(y_1, y_2, ..., y_n) = v$$
and using knowledge of his trapdoor he gets x_k from y_k.
5. **Output the ring signature** : The ring signature on message m is defined to be the $(2r + 1)$ tuple:
$$(P_1, P_2, ..., P_r; v; x_1, x_2, ..., x_r)$$

Ring signature verification: On receiving $(P_1, P_2, ..., P_r; v; x_1, x_2, ..., x_r)$ as the ring signature on message m, the verifier can verify as follows.

1. **Apply trapdoor permutation** : verifier computes for each i, $y_i = g_i(x_i)$
2. **Key computation** : computes $k = h(m, P_1, P_2, ..., P_r)$
3. **Verify the ring equation** : The verifier checks if

$$C_{k,v}(y_1, y_2, ..., y_n) = v$$

   If the ring equation is satisfied, the verifier accepts the signature as valid otherwise rejects.

3 Bilinear Pairings

Let $\mathbf{G}_1$ cyclic additive group generated by P, whose order is a prime q, and G2 be a cyclic multiplicative group of the same order q: A bilinear pairing is a map $e : \mathbf{G}_1 \times \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ with the following properties:
P1: *Bilinear*: $e(aP, bQ) = e(P, Q)^{ab}$;
P2: *Non-degenerate*: There exists $P, Q \in \mathbf{G}_1$ such that $e(P, Q) \neq 1$;
P3: *Computable*: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbf{G}_1$.

When the DDHP (Decision Diffie-Hellman Problem) is easy but the CDHP (Computational Diffie-Hellman Problem) is hard on the group G; we call G a Gap Diffie-Hellman (GDH) group. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over a finite field, and the bilinear parings can be derived from the Weil or Tate pairing. [1, 4, 7]

4 Proposed ID-based Ring Signature Scheme (IDBRS)

Setup : Let P is a generator of $\mathbf{G}_1$; $e : \mathbf{G}_1 \times \mathbf{G}_1 \longrightarrow \mathbf{G}_2$ is a bilinear pairing. $H_1 : \{0,1\}^* \longrightarrow z_q^*$, $H_2 : \{0,1\}^* \longrightarrow \mathbf{G}_1$ and $H_3 : \mathbf{G}_2 \longrightarrow z_q^*$ are cryptographic hash functions. Key Generation Center (KGC) chooses a random number $s \in Z_q^*$ and sets $P_{Pub} = sP$. The KGC publishes the system parameters $\{G_1, G_2, e, q, P, P_{Pub}, H_1, H_2\}$ and keeps s as the master key.

Extract : An user submits its identity information ID_k to KGC. KGC publishes the public key $Q_k = H_2(ID_k)$ and returns $S_k = sQ_k$ to the user as his/her private key.

Ring signature generation: Given a message m to be signed, signer's secret key S_k, and the possible signers' public keys sequence $L = (ID_1, ID_2, ..., ID_r)$ of all ring members, the signer computes the ring signature as follows.

1. **Choose a key** : $K = H_1(m||L)$.

2. **Pick a random glue value** : The signer picks a random $A \in G_1$ and computes the initialization value
$$v = c_k = e(A, P)^K$$
3. **Pick random T_i's** : The signer picks a random T_i for all other ring members uniformly and independently from G_1, and computes
$$c_{i+1} = [e(P_{Pub}, H_3(c_i)Q_i).e(T_i, P)]^K$$
.
4. **Formation of ring** : The signer solves the ring equation for y_k. when $i = k$, we get
$$c_{k+1} = [e(P_{Pub}, H_3(c_k)Q_k).e(T_k, P)]^K = v$$
On solving this ring equation we get
$$T_k = A - H_3(c_k)S_k$$
Now compute $T = \Sigma\ T_i$
5. **Output the ring signature** : The ring signature on message m is the tuple
$$(L; c_1, c_2, ..., c_r; T)$$

Ring signature verification: On receiving the ring signature $(L; c_1, c_2, ..., c_r; T)$ on message m, the verifier can verify as follows. The verifier computes
$$K = H_1(m||L).$$
and checks if
$$\Pi_i c_i = [e(P_{Pub}, \Sigma_i(H_3(c_i)Q_i)).e(T, P)]^K$$
If the equation is satisfied, the verifier accepts the signature as valid otherwise rejects.

5 Analysis of IDBRS

5.1 Correctness

From ring signature generation protocol –
$$c_{i+1} = [e(P_{Pub}, H_3(c_i)Q_i).e(T_i, P)]^K$$
$$\Pi_{i=0}^{r} c_{i+1} = \Pi_{i=0}^{r}[e(P_{Pub}, H_3(c_i)Q_i).e(T_i, P)]^K$$
$$\Pi_{i=0}^{r} c_{i+1} = [\Pi_{i=0}^{r} e(P_{Pub}, H_3(c_i)Q_i).\Pi_{i=0}^{r} e(T_i, P)]^K$$
$$\Pi_{i=0}^{r} c_{i+1} = [e(P_{Pub}, \Sigma_{i=0}^{r}(H_3(c_i)Q_i)).e(\Sigma_{i=0}^{r} T_i, P)]^K$$
$$\Pi_i c_i = [e(P_{Pub}, \Sigma_i(H_3(c_i)Q_i)).e(T, P)]^K$$
which hold true, since we have $c_{r+1} = c_0$

5.2 Security

The proposed ID-based ring scheme holds unconditionally signer-ambiguity, as all T_i but T_k are taken randomly from G_1: In fact, at the starting point, the T_k is also distributed uniformly over G_1, since A is randomly chosen from G_1. We fix a set of identities, denoted by L.

Suppose that $\mathcal{A}$ is an adversary whose identity ID_A is not listed in L, but he wants to forge a valid ring signature. $\mathcal{A}$ can either forge a valid signature of a user whose identity ID_k is listed in L or executes the following experiment:

1. $\mathcal{A}$ queries `Extract` q_E , ($q_E > 0$) times with known parameters and ID_i, which does not not belongs to L,for $i = 1, 2, ..., q_E$. The query `Extract` returns the q_E corresponding secret key such that $S_i = sH_2(ID_i) = sQ_i$.
2. He Chooses randomly an integer $c_0 \in Z_q^*$
3. He runs ring signature generation protocol's third step for $i = 0, 1, ..., r - 2$, where $r = |L|$
4. Assigns $c_0 = [e(P_{Pub}, H_3(c_{k-1})Q_{k-1}).e(T_{k-1}, P)]^K$
5. Outputs the ring signature $(L; c_1, c_2, ..., c_r; T)$

After running Step 1 of the above experiment, $\mathcal{A}$ gets $\{S_1, S_2, ..., S_{q_E}\}$, a set of secret keys . Suppose he gets a pair (ID_m, S_m) such that $H_2(ID_m) = H_2(ID_j)$, where $ID_J \in L$, then he can forge a valid ring signature. But since H_2 is random oracle and `Extract` generates random numbers with uniform distributions. This implies that $\mathcal{A}$ gets nothing from query results. H_3 is random oracle and all Ti are taken randomly from G_1. This implies that the probability of $c_0 = [e(P_{Pub}, H_3(c_{k-1})Q_{k-1}).e(T_{k-1}, P)]^K$ to be true is $\frac{1}{q}$. So we can say that the proposed scheme is non-forgeable.

5.3 Efficiency

The proposed ring signature scheme works under the environment of supersingular elliptic curves or hyperelliptic curves. The essential operation in our ID-based signature schemes is to compute a bilinear pairing.

We denote by P, the cost of computation a bilinear pairing, A_{G_1} the cost of addition in G_1, M_{G_1} cost of multiplication in G_1, M_{G_2} cost of multiplication in G_2 and cost of multiplication in Z_q by M_{Z_q}. The cost of hashing is denoted by H. We shall not consider exponentiation as it can be reduced in addition in G_1. We ignore the cost of computation of $H_2(ID)$

In our opinion both the first two schemes discussed in **Table 1** are having inconsistency in the computational procedure. As in Zhang's scheme [16], in initialization, $c_{k+1} = H(L||m||e(A, P))$ has been computed, which is incorrect. H is defined in their paper as $H : \{0, 1\}^* \rightarrow Z_q$. But in computation of c_{k+1}, the pairing $e(A, P)$ had used, which belongs to V (according to their notation), not to Z_q. This shows their c_{k+1} computation is taken incorrectly. We may remove this inconsistency by applying a newly defined hash function as $H_4 : G_2 \rightarrow \{0, 1\}^*$. If we modify their scheme's in this way, computational cost of their scheme

Table 1. Comparison of computational cost with existing schemes.

	Signature Generation	Verification
Zhang's Scheme	$(2n-1)P + nH + nA_{G_1}$ $+nM_{G_1} + (n-1)M_{G_2}$	$2nP + nH + nM_{G_1} + nM_{G_2}$
Lin's Scheme	$(2n-1)P + H + nA_{G_1}$ $+(2n-1)M_{G_1} + nM_{G_2}$	$2P + H + (n-1)A_{G_1}$ $+(n+1)M_{G_1} + nM_{G_2}$
Proposed Scheme	$(2n-1)P + nH + (n+1)A_{G_1}$ $+2nM_{G_1} + (n-1)M_{G_2}$	$2P + (n+1)H + (n+1)A_{G_1}$ $+(n+1)M_{G_1} + (n-1)M_{Z_q} + M_{G_2}$

increases by a factor nH in signature phase and by a factor of nH in verification phase. A very similar mistake is in Lin's scheme [12] is made. In Equation 3, they have computed $c_{a+1} = e(A, P)$. This implies that the c_{a+1} is an element of G_2, but they have treated it as element of Z_q in equation 4 and also in equation 5. (If $P \in G_2$ and $Q \in G_1$ then $P.Q$ is not defined.). If we define a hash function $H_5 : G_2 \rightarrow Z_q$, computational cost of this scheme is also increased by a factor nH in signature generation phase and also nH in verification phase. Our scheme does not contain such inconsistency and also is more efficient.

6 ID-based Proxy Ring Signature Scheme (IDBPRS)

6.1 Delegation Function due to Zhang et al. [17]

Here an original signer with secret key- public key pair (x_o, PK_o) wants to delegate signing power to proxy signer with secret key- public key pair (x_p, PK_p). System parameters are $\{G_1, G_2, e, q, P, H_1, H_2\}$. The original signer runs the following protocol -

- The original signer prepares a warrant message consist of explicit description of the delegation relation. warrant message also contains some identity information of the proxy signer.
- The original signer computes $x_{ow} = x_o H_2(w)$ and sends (x_{ow}, w) to the proxy signer.
- Proxy signer checks $e(x_{ow}, P) = e(H_2(w), PK_o)$. If it holds, he computes then $x_w = x_{ow} + x_p H_r(w)$.

Above protocol can be regarded as **PKGen** (Proxy key generation protocol) in proxy signature scheme. In this delegation proxy signer will use x_w as secret key and $PK_o + PK_p$ as public key. Now proxy signer may use any ID-based signcryption scheme from pairing (takes the ID public key as $H_2(w)$ and secret key x_w and the public key of trusted authority as $PK_o + PK_p$) to get proxy signcryption scheme. Security of above protocol is discussed in [17].

7 A New Proxy Ring Signature Scheme from Pairings

[Setup] The system parameters `params` $= \{\mathbf{G}_1, \mathbf{G}_2, e, q, P, H_1, H_2\}$ Let Alice be the original signer with public key $PK_o = s_o P$ and private key s_o, and

$L = \{PS_i\}$ be the set of proxy signers with public key $PK_{p_i} = s_{p_i}P$ and private key s_{p_i}.

[Proxy Key Generation] The original signer prepares a warrant w, which is explicit description of the delegation relation. Then he sends $(w, s_oH_2(w))$ to the proxy group L. Each proxy signer uses his secret key S_{p_i} to sign the warrant w and gets his proxy key $S_i = s_oH_2(w) + s_{p_i}H_2(w)$.

[Proxy Ring Signing]For signing any message m, the proxy signer PS_i chooses a subset $L' \subseteq L$. Proxy signers's public key is listed in L'. Now to sign he/ she perform following operations:

- **Initialization**: Choose randomly an element $A \in \mathbf{G}_1$, compute
$$c_{k+1} = e(A, P) \tag{1}$$
- **Generate forward ring sequence** For $i = k+1, k+2, ...k+(n-1)$ choose randomly $T_i \in \mathbf{G}_1$ and compute
$$c_{i+1} = e(PK_o + PK_{p_i}, H_3(c_i)H_2(w))^{H_2(m\|L)}.e(Ti, P) \tag{2}$$
- **Forming the ring**: Let $R_n = R_o$. Then, PS_i computes
$$T_i = A - h_2(m \parallel L)H_3(c_i)S_i, \tag{3}$$
$$T = \Sigma_{i=1}^{n} T_i \tag{4}$$
- **Output**: Finally, Let $c_n = c_0$. The resulting ring signature for a message m and with ring member specified by L' is the $(n+1)$-tuple:$(c_1, c_2, ..., c_n, T)$

[Verification] Given message m, its ring signature $(c_1, c_2, ..., c_n, T)$, and the set L' of the identities of all ring members, the verifier can check the validity of the signature by the testing if:

$$\Pi_{i=1}^{n} c_i = e(PK_o + PK_{p_i}, \Sigma_{i=1}^{n} H_3(c_i)H_1(w))^{H_2(m\|L)}.e(T, P) \tag{5}$$

8 Analysis

Key Secrecy In computing user P_i's private key S_i from the corresponding public key $PK_o + PK_{P_i}$ requires the knowledge of original signer's private key s_o and proxy signer's private key s_{p_i}. According to definition these keys are protected under the intractability of DLP in G_1 as $PK_o = s_oP$ and $PK_{P_i} = s_{p_i}P$.

Signer ambiguity In a valid proxy ring signature $(c_1, c_2, ..., c_n, T)$ with proxy group L' generated by PS_i all c_i's are computed by eq 2. Since $T_i \in G_1$ is chosen uniformly at random, each c_i is uniformly distributed over G_2. Thus, regardless who the actual signer is and how many ring members involved $(c_1, c_2, ..., c_n)$ biases to no specific ring member. Other discussion are very similar as in previous sections.

9 Conclusion

In this paper we proposed a new ID-based ring signature scheme from bilinear pairings. This scheme removes deficiencies in existing schemes. In this paper we proposed a new and a proxy ring signature scheme which, whenever proxy signer want to sign message on behalf of the original signer provide anonymity. The proposed scheme is more efficient than the scheme of Zhang et al.'s, especially for the pairing operation required in the signature verification. This proxy ring signature scheme is more efficient for those verifiers who have limited computing power.

References

1. D. Boneh and M. Franklin, *Identity-based encryption from weil pairing*, Advances in Cryptology - Crypto 2001 **LNCS 2139** (2001), 213–229.
2. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from weil pairing*, Advances in Cryptology - Asiacrypt 2001 **LNCS 2248** (2001), 514–532.
3. X. Boyen, *Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography*, Advances in Cryptology- Crypto 2003 **LNCS 2729** (2003), 382–398.
4. J. C. Cha and J. H. Cheon, *An identity-based encryption from gap diffie-hellman groups*, Public Key Cryptography - PKC 2003 **LNCS 2139** (2003), 18–30.
5. J. Cheon and J. Cha, *Identity-based signature from the weil pairings*, (2001), Available at http://vega.icu.ac.kr/∼jhcheon/publicaion.html.
6. F. Hess, *Exponent group signature schemes and efficient identity based signature scheme based on pairings*, Tech. Report No. 2002/012, Cryptology ePrint Archive.
7. ______, *Efficient identity-based signture schemes based on pairings*, SAC 2002 **LNCS 2595** (2002), 310–324.
8. S. J. Hwang and C. H. Shi, *A simple multi-proxy signature scheme*, Proceedings of the 10th National Conference on Infroation Security, Taiwan (2000), 134–138.
9. S. Kim, S. Park, and D. Won, *Proxy signatures, revisited*, Proc. of ICICS 97 **LNCS 1334** (1997), 223–232.
10. S. Lal and A. K. Awasthi, *Proxy blind signature scheme*, Cryptology ePrint Archive, Report 2003/072, 2003, http://eprint.iacr.org/.
11. J. Y. Lee, J. H. Cheon, and S. Kim, *An analysis of proxy signatures: Is secure channel neccessary?*, CT-RSA 2003 **LNCS 2612** (2003), 68–79.
12. C. Y. Lin and T. C. Wu, *An identity-based ring signature scheme from bilinear pairings*, Cryptology ePrint Archive, Report 2003/117, 2003, http://eprint.iacr.org/.
13. A. Shamir R. Rivest and Y. Tauman, *How to leak secret*, In Asiacrypt'01 **LNCS 2248** (2001), 552–565.
14. A. Shamir, *Identity-based cryptosystems and signature schemes*, Proc. of Crypto 84 **LNCS 196** (1985), 47–53.
15. C. Y. Chang W. B. Lee, *Effiecient proxy-protected proxy signature scheme based on discrete logarithm*, Proceeding of 10th Conference on Information Security, Hualien, Taiwan, (2000), 4–7.
16. F. Zheng and K. Kim, *Id-based blind signature and ring signature from pairings*, Advances in cryptology Asiacrypt 2002 **LNCS 2501** (2002), 533–547.
17. F. Zheng, R. S. Naini, and C. Y. Lin, *New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings*, Tech. Report 2003/0..., Cryptology ePrint Archive, available at: http://eprint.iacr.org/2003/, 2003.