

A New Proxy Ring Signature Scheme

Amit K Awasthi¹ and Sunder Lal²

¹ Hindustan College of Science and Technology,
Farah, Mathura - 281122 UP - INDIA
awasthi_hcst@yahoo.com

² Institute of Basic Sciences,
Khandari, Agra - 282002(UP) - INDIA

Abstract. The concept of ring signature was introduced by Rivest, Shamir and Tauman. This signature is considered to be a simplified group signature from which identity of signer is ambiguous although verifier knows the group to which signer belong. In this paper we introduce a new proxy ring signature scheme.¹

Keywords: ID-based Signature Schemes, Proxy Signature, Ring Signature, Proxy Ring Signature

1 Introduction

Consider the following situation discussed by Zhang et al. in [10]-

An entity delegate his signing capability to many proxies, called proxy signers set. Any proxy signer can perform the signing operation of the original entity. These proxy signers want to sign messages on behalf of the original entity while providing anonymity. Of course, this problem can be solved by group signature (Take the group manager as the original entity). But in some applications, it is necessary to protect the privacy of participants (we believe that unconditional anonymity is necessary in many occasions). If the proxies don't hope that some one (include the original signer) can open their identities, the group signature is not suitable in here (Because a group manager can open the signature to reveal the identity of the signer).

To solve above problem proxy ring signature scheme was introduced by Zhang et al [10]. In this paper, we propose a new proxy ring signature

¹ This paper appeared at the conference 'RMS 2004', Agra, INDIA

scheme based on Lin-Wu's [9] ID-based ring signature scheme from bilinear pairing. As compared to previous scheme [10], our scheme is computationally more efficient, especially for the pairing operations required during signature verification.

2 Preliminaries

– Bilinear Pairings

Let \mathbf{G}_1 cyclic additive group generated by P , whose order is a prime q , and \mathbf{G}_2 be a cyclic multiplicative group of the same order q : A bilinear pairing is a map $e : \mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$ 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 finite field, and the bilinear pairings can be derived from the Weil or Tate pairing. We can refer to [7,10] for more details.

Through this paper, we define the system parameters in all schemes are as follows: Let P be a generator of \mathbf{G}_1 ; the bilinear pairing is given by $e : \mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_2$. Define two cryptographic hash functions $H_1 : \{0, 1\}^* \rightarrow \mathbf{Z}_q$ and $H_2 : \{0, 1\}^* \rightarrow \mathbf{G}_2$.

- **Pairing based short signature scheme (PBSSS)** Boneh et al.'s pairing based short signature scheme is as follows-

Key Generation Choose a random number $s \in \mathbf{Z}_q^*$ and compute $P_{Pub} = sP$ where $(G_1, G_2, q, P, P_{Pub}, H_2)$ are public parameter and s is the secret key.

Signing For a message $m \in \{0, 1\}^*$, compute $P_m = H_2(m) \in \mathbf{G}_2$. Then $S_m = sP_m$ is the signature on message m .

Verification Check whether the following equation holds

$$e(S_m, P) = e(H_2(m), P_{Pub})$$

This scheme is proven to be secure against existential forgery on adaptive chosen message attack (in random oracle model) assuming Computationally Diffie Hellman Problem is hard [8].

3 Proposed Scheme

[Setup] The system parameters $\text{params} = \{\mathbf{G}_1, \mathbf{G}_2, e, q, P, H_1, H_2\}$ 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 $(w, s_o H_2(w))$ 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 $S_i = s_o H_2(w) + s_{p_i} H_2(w)$.

[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

$$c_{k+1} = e(A, P) \quad (1)$$

- Generate forward ring sequence For $i = k + 1, k + 2, \dots, k + (n - 1)$ choose randomly $T_i \in \mathbf{G}_1$ and compute

$$c_{i+1} = e(PK_o + PK_{p_i}, c_i H_2(w))^{H_2(m \| L)}.e(T_i, P) \quad (2)$$

- Forming the ring: Let $R_n = R_o$. Then, PS_i computes

$$T_i = A - h_2(m \| L) c_i S_i, \quad (3)$$

$$T = \sum_{i=1}^n T_i \quad (4)$$

- 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: $(c_1, c_2, \dots, c_n, T)$

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

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

4 Performance and Security Discussion

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 $(c_1, c_2, \dots, c_n, T)$ 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, \dots, c_n) biases to no specific ring member.

5 Conclusion

In this paper we proposed a new proxy ring signature which becomes needful whenever proxy signer want to sign message on behalf of the original signer providing anonymity. The proposed scheme is more efficient as compared with the 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. Mambo, M., Usuda, K., Okamoto, E.: Proxy Signature: Delegation of the power to sign messages, IEICE Trans. Fundamentals, E79-A:9, (1996) 1338 - 1353 5.
2. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures for delegating signing operation, Proc. 3rd ACM Conference on Computer and Communication Security, (1996) 48-57
3. Kim, S., Park, S., Won, D.: Proxy signatures: Revisited, ICICS'97, LNCS Vol. 1334, Springer-Verlag, (1997) 223-232
4. Lee, W. B., Chang, C. Y.: Efficient Proxy-protected proxy signature scheme based on discrete logarithm, Proceedings of 10th Conference on Information Security, Hualien, Taiwan, ROC, (2000) 4-7
5. M. Abe, M. Ohkubo, and K. Suzuki, 1-out-of-n signatures from a variety of keys, To appear in Advances in Cryptology-Asiacrypt 2002, 2002.
6. P.S.L.M. Barreto, H.Y. Kim, B.Lynn, and M.Scott, Effient algorithms for pairing-based cryptosystems, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
7. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
8. D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

9. C. Y. Lin and T. C. Wu, An Identity-based Ring Signature Scheme form Bilinear Pairings, Cryptology ePrint Archive, Report 2003/117 available at <http://eprint.iacr.org/2003/117/>.
10. F. Zhang, R. S. Naini and C Y Lin, New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings, Cryptology ePrint Archive, Report 2003/117 available at <http://eprint.iacr.org/2003/104/>.
11. F. Zhang and K. Kim, ID-based Blind Signature and Ring Signature from Pairings, Advances in Cryptology, Asiacrypt 2002, LNCS 2501, Springer-Verlag, pp 533-547.