An identity-based ring signature scheme from bilinear pairings

Chih-Yin Lin and Tzong-Chen Wu*
Institute of Information Management, National Chiao Tung University, Taiwan
Email: lincy@iim.nctu.edu.tw
*Department of Information Management,
National Taiwan University of Science and Technology, Taiwan
Email: tcwu@cs.ntust.edu.tw

Abstract

At the conference Asiacrypt 2001, Rivest, Shamir and Tauman firstly addressed the concept of ring signature. In this paper we propose an identity-based ring signature scheme from bilinear pairings. As compared with the Zhang-Kim scheme (presented at the conference Asiacrypt 2002), our scheme is more efficient in computation and requires fewer pairing operations.

Keywords: ring signature, identity-based, bilinear pairings.

1. Introduction

At the conference Asiacrypt 2001, Rivest, Shamir and Tauman [1] firstly addressed the concept of ring signature. A ring signature can be considered as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism against signer's anonymity. In a ring signature scheme, the information of all possible signers, i.e. ring members, serves as a part of the ring signature for the signed message. A valid ring signature will convince the verifier that the signature is generated from one of the ring members, without revealing any information about which ring member is the actual signer. Herein, the anonymous property is referred to as signer-ambiguity. Applications of ring signatures include leaking secrets and authenticated communication [1].

Recently the bilinear pairings have been found advantageous in designing various cryptographic schemes, especially for those using identity-based public keys, e.g. the identity-based encryption [2] and the identity-based signature [3]. For all these schemes, the performance heavily depends on the cost of computing pairing operations. Therefore, many efforts such as [4-5] have been focused on speeding up the computation of pairings. Although significant results have been proposed [4-5], it is still important to design new schemes that require less pairing operations to achieve better performance.

In this paper, we will propose an identity-based ring signature scheme from bilinear pairings. As compared with the Zhang-Kim scheme ([6], presented at the conference Asiacrypt 2002), our scheme is computationally more efficient, especially for the pairing operations required during signature verification. In below, the bilinear pairing is introduced. Then, we will propose our scheme and give discussions and analysis.

2 Bilinear pairing

Assume G_1 is an additive cyclic group of prime order q; and, G_2 is a multiplicative cyclic group of prime order q. As in [2-6], G_1 can be considered as a subgroup of points on an elliptic curve over a finite field; and, G_2 a subgroup of the multiplicative group of a related finite field. The bilinear pairing $e: G_1 \times G_1 \to G_2$ has the following properties:

i) *Bilinear*: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$.

ii) *Non-degenerate*: There exists a $P \in G_1$, such that $e(P, P) \neq 1$.

iii) *Computable*: Given $P,Q \in G_1$, there is an efficient algorithm to compute $e(P,Q)$.

As specified in [2-6], the decisional Diffie-Hellman problem (DDHP) in G_1 should be easy. The DDHP in G_2, the computational Diffie-Hellman problem (CDHP) and the discrete logarithm problem (DLP) in both G_1 and G_2 should be hard. The inversion of the bilinear pairing should be hard, i.e. the bilinear pairing inversion problem (BPIP), which is defined as:

- BPIP: Given $P \in G_1$ and $e(P,Q) \in G_2$, find $Q \in G_1$.

As analyzed in [7], BPIP is reducible from CDHP in G_2 and can be reduced to DLP in G_2. Such bilinear pairing *e* has been successfully realized on certain elliptic curves, such as the modified Weil pairing [2] and Tate pairing [4-5].

3 Proposed scheme

Assume there is a trusted key generation center (TKGC) that will establish the identity-based cryptosystem and generate private keys for users. Initially, TKGC selects *q*, G_1, G_2, and *e*, as defined in the previous section. Then, TKGC selects $P \in G_1$ as the generator of G_1 and defines one-way hash function $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \to Z_q$. TKGC's private key is $s \in Z_q^*$ and the public key is $P_{pub} \in G_1$, computed as:

$$P_{pub} = sP . \quad \text{EQ.1}$$

Finally, TKGC keeps *s* secretly and publishes $\{G_1, G_2, q, e, P, P_{pub}, H_1, H_2\}$. The proposed scheme consists of three phases: **key generation**, **ring signature generation**, and **ring signature verification**, stated as follows.

<**Key generation**> For each signer u_i in the system, TKGC generates u_i's private key D_i based on u_i's unique identity ID_i, as:

$$D_i = sH_1(ID_i) . \quad \text{EQ.2}$$

<**Ring signature generation**> Without loss of generality, assume there are *n* members $u_1, u_2, ..., u_n$ in the ring chosen by the actual signer u_a, $1 \le a \le n$. Given the message *m* to be signed, u_a firstly prepares a set *L* of the unique identities from all ring members, i.e. $L = \{ID_1, ID_2, ..., ID_n\}$. Then, u_a selects $A \in G_1$ at random and computes c_{a+1} as:

$$c_{a+1} = e(A,P) . \quad \text{EQ.3}$$

In accordance with the order of *i*=*a*+1, *a*+2, …, *a*+(*n*-1) (mod *n*), u_a randomly selects $R_i \in G_1$, and computes c_{i+1} as:

$$c_{i+1} = e(P_{pub}, c_i H_1(ID_i))^{H_2(m \| L)} \cdot e(R_i, P) . \quad \text{EQ.4}$$

Let $R_n = R_0$. Then, u_a computes R_a and *R* as:

$$R_a = A - H_2(m \| L) c_a D_a , \quad \text{EQ.5}$$

$$R = \sum_{i=1}^{n} R_i . \quad \text{EQ.6}$$

Finally, let $c_n = c_0$. $(c_1, c_2, ..., c_n, R)$ is the ring signature for message *m* with ring members specified by *L*.

<**Ring signature verification**> Given message *m*, its ring signature $(c_1, c_2, ..., c_n, R)$, and the set *L* of identities of all ring members, the verifier can check the validity of the signature by testing if:

$$\prod_{i=1}^{n} c_i = e(P_{pub}, \sum_{i=1}^{n} c_i H_1(ID_i))^{H_2(m \| L)} \cdot e(R, P) . \quad \text{EQ.7}$$

4 Security analysis

We consider three security requirements to the proposed scheme: key secrecy, unforgeability and

signer-ambiguity. In below, we will give their definitions and show that the proposed scheme achieves them under the intractability of DLP and BPIP.

- Key secrecy: Given all public information, deducing signer u_i 's private key D_i is computationally infeasible.
- Unforgeability: Given a message *m*, a set *L* of identities of ring members, and all public information, any $u_k \notin L$ cannot compute a valid ring signature that satisfies EQ.7.
- Signer-ambiguity: Given message *m*, its ring signature $(c_1, c_2, ..., c_n, R)$, and the set of ring members $L = \{ID_1, ID_2, ..., ID_n\}$, it is unconditionally infeasible to find out who is the actual signer.

<Achievement of key secrecy> In the proposed scheme, all signers' private keys are generated by EQ.2. Thus, computing u_i 's private key D_i from the corresponding public key $H_1(ID_i)$ requires the knowledge of TKGC's private key *s*. As defined in EQ.1, *s* is protected under the intractability of DLP in G_1. Moreover, if the adversary assumes u_a, $1 \le a \le n$, is the actual signer for ring signature $\{L = \{ID_1, ID_2, ..., ID_n\}, (c_1, c_2, ..., c_n, R), m\}$ and intends to compute u_a 's private key D_a from EQ.5. The adversary will have to know *A* for such attack. By EQ.3, he will face the intractability of BPIP to obtain *A*. Therefore, due to DLP in G_1 and BPIP, key secrecy is assured.

<Achievement of unforgeability> Given the set $L = \{ID_1, ID_2, ..., ID_n\}$ of all ring members, an adversary $u_k \notin L$ may try to compute a valid ring signature for message *m* via two ways. First, he randomly chooses the values of $(c_1, c_2, ..., c_n)$ and tries to compute *R* such that $(c_1, c_2, ..., c_n, R)$ will satisfy EQ.7. Computing such *R* is equivalent to solving it in $e(R, P) = \alpha$, where $\alpha = (\prod_{i=1}^{n} c_i) \cdot e(P_{pub}, \sum_{i=1}^{n} c_i H_1(ID_i))^{-H_2(m\|L)}$. This will lead to the BPIP intractability. Second, w.l.o.g the adversary chooses $(c_2, ..., c_n, R)$ at random and then tries to compute c_1 such that $(c_1, c_2, ..., c_n, R)$ will satisfy EQ.7. Computing such c_1 is equivalent to solving it in $c_1 = y \cdot z^{c_1}$, where $y = (\prod_{i=2}^{n} c_i)^{-1} \cdot e(P_{pub}, \sum_{i=2}^{n} c_i H_1(ID_i))^{H_2(m\|L)} \cdot e(R, P)$ and $z = e(P_{pub}, H_1(ID_1))^{H_2(m\|L)}$, which as a result is the intractable DLP in G_2. Therefore, due to DLP in G_2 and BPIP, unforgeability is achieved.

<Achievement of signer-ambiguity> In a valid ring signature $(c_1, c_2, ..., c_n, R)$ with $L = \{ID_1, ID_2, ..., ID_n\}$ generated by u_a, $1 \le a \le n$, all c_i 's, $i \ne a+1$, are computed by EQ.4. Since $R_i \in G_1$ is chosen uniformly at random, each c_i is uniformly distributed over G_2, for all $i \ne a$. As for the starting point of the ring, c_a is computed by EQ.3. Because *A* is also chosen uniformly at random, c_a 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.

5 Efficiency

The computational costs required are considered in terms of the notations: *Pa* the pairing, MuG_1 the multiplication in G_1, AdG_1 the addition in G_1, MuG_2 the multiplication in G_2, and *Ha* the hash function computation. Notice that the cost for computing an exponentiation in G_2 is evaluated herein as a multiplication in G_1 and we ignore the cost of computing $H_1(ID_i)$.

Table 1 shows the costs in ring signature generation and verification of the proposed scheme, and the comparison with Zhang-Kim's scheme [6]. We also consider possible pre-computations for signature generation that are indirectly relevant to the message signing, e.g. EQ 3. and EQ.6.

Consequently, we can see that the proposed scheme has comparable performance with Zhang-Kim's scheme for signature generation. As for signature verification, the proposed scheme requires only two pairing computations while Zhang-Kim needs 2*n*. If we consider the complexity instead of the exact number of operations as seen in Table 1, the comparison is more significant. For

signature generation, Pa, MuG_1 and MuG_2 are O(n), and Ha and AdG_1 are O(1) in our scheme, while these measures are all O(n) in [6]. For signature verification, Pa and Ha are O(1) in our scheme, while they are O(n) in [6].

Table 1 –
Computational costs for the proposed scheme and the Zhang-Kim scheme ($\boldsymbol{n}$ ring members)

	Signature generation	Signature generation (with pre-computation)	Verification
Proposed scheme	$(2\boldsymbol{n}\text{-}1)Pa+Ha+$ $\boldsymbol{n}\ AdG_1+(2\boldsymbol{n}\text{-}2)\ MuG_1$ $+\boldsymbol{n}\ MuG_2$	$(\boldsymbol{n}\text{-}1)Pa+Ha+\ AdG_1+$ $(2\boldsymbol{n}\text{-}2)\ MuG_1+\boldsymbol{n}\ MuG_2$	$2Pa+Ha+(\boldsymbol{n}\text{-}1)\ AdG_1+$ $(\boldsymbol{n}+1)\ MuG_1+\boldsymbol{n}\ MuG_2$
Zhang-Kim	$(2\boldsymbol{n}\text{-}1)Pa+\boldsymbol{n}Ha$ $+\boldsymbol{n}\ AdG_1+\boldsymbol{n}\ MuG_1$ $+(\boldsymbol{n}\text{-}1)\ MuG_2$	$\boldsymbol{n}Pa+\boldsymbol{n}Ha+\boldsymbol{n}\ AdG_1+$ $\boldsymbol{n}\ MuG_1+(\boldsymbol{n}\text{-}1)\ MuG_2$	$2\boldsymbol{n}Pa+\boldsymbol{n}Ha+$ $\boldsymbol{n}\ MuG_1+\boldsymbol{n}\ MuG_2$

6 Conclusions

In this paper, we have proposed a new ID-based ring signature scheme from bilinear pairings. The proposed scheme is more efficient as compared with the Zhang-Kim scheme, especially for the pairing operations required in signature generation. For the applications of ring signatures, such as authenticated communication, the proposed scheme is more suitable for those verifiers who only have limited computing power.

References

1. RIVEST, R., SHAMIR, A., and TAUMAN, Y.: 'How to leak a secret', *Advances in Cryptology – Asiacrypt 2001*, LNCS 2248, Springer-Verlag, 2001, pp. 552-565.
2. BONEH, D., and FRANKLIN, M.: 'Identity-based encryption from the Weil pairing', *Advances in Cryptology – Crypto 2001*, LNCS 2139, Springer-Verlag, 2001, pp. 213-229.
3. PATERSON, K. G.: 'An identity-based signature from pairings on elliptic curves', *Electronics Letters*, 2002, 38(2), pp. 1025-1026.
4. BARRETO, P. S. L. M., KIM, H. Y., LYNN, B., and SCOTT, M.: 'Efficient Algorithms for Pairing-Based Cryptosystems', *Advances in Cryptology – Crypto 2002*, LNCS 2442, Springer-Verlag, 2002, pp. 354-368.
5. GALBRAITH, S. D., HARRISON, K., and SOLDERA, D.: 'Implementing the Tate pairing', *Algorithmic Number Theory Symposium – ANTS-V*, LNCS 2369, Springer-Verlag, 2002, pp. 324-337.
6. ZHANG, F., and KIM, K.: 'ID-based blind signature and ring signature from pairings', *Advances in Cryptology – Asiacrypt 2002*, LNCS 2501, Springer-Verlag, 2002, pp. 533-547.
7. YACOBI, Y.: 'A note on the bi-linear Diffie-Hellman assumption', *IACR Cryptology ePrint Archive*, Report 2002/113, 2002.