

Two ID-Based Analogous Ring Signature Schemes^{*}

ZHANG Jian-Hong^{1†} WANG Ji-Lin² WANG Yu-Min²

(1 *Science College, North China University of Technology, Beijing 100041, China;*

2 *National Key Lab. of ISN, Xidian University, Xi'an 710071, China*)

(Received 10 December 2002; Revised 1 September 2003)

Zhang JH, Wang JL, Wang YM. Two ID-based analogous ring signature schemes. *Journal of the Graduate School of the Chinese Academy of Sciences*, 2005, 22(1): 78~82

Abstract This paper presents two ID-based analogous ring signature schemes in which any user can sign on behalf of the set to which he belongs, but a verifier can't tell which member actually produced the digital signature. For an attacker, even if he had known all the secret signing keys, he couldn't have identified the actual signer. In this paper our proposed schemes realize unconditional anonymity.

Key words analogous ring signature, identity, unconditional security

CLC TP309

1 Introduction

Digital signature, one of the most important applications of public key cryptosystem, can be used to protect data integrity and authenticate the identity of the sender of a message. It plays an important role in the electronic transactions. However, in some cases such as anonymous votes and anonymous bids, we need to sign a document without revealing our identity.

Identity-based cryptosystem is a novel type of cryptographic scheme proposed by Shamir^[1], which enables any pair of users to communicate securely, and to verify each other's signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party. Problems with the traditional Public key cryptosystems (PKCs) are the high cost of the infrastructure needed to manage and authenticate public keys, and the difficulty in managing multiple communities. Whilst ID-based PKCs will not replace the conventional Public Key infrastructures, it might prove to be a complementary technology.

In an ID-based PKC, everyone's public keys are predetermined by information that uniquely identifies them, such as their email addresses. There is no need for any public key certificate. A trusted key generation centre (KGC) generates the private keys of the entities in the group using their public key. In 1984, Shamir^[2] proposed the idea of identity-based cryptosystems. While the ID-based signature schemes have satisfactory solutions, the first practical ID-based encryption scheme was that of Boneh and Franklin in 2001. Several other ID-based schemes were proposed based on Boneh-Franklin's scheme.

Generally, we can realize anonymity by group signature. Most of ID-based group signatures are insecure such

^{*} supported by the National Natural Science Foundation of China(G69931010)

[†] E-mail: jhzhs@eyou.com

as Ref. [2, 3]. In this paper, we present two efficient ID-based signature schemes in which the signer is ambiguous; a verifier does not learn who the actual signer is, but only proves that he belongs to a certain set of possible members. The similar notion of “ring signature” was introduced in 2001 by Ronald L. Rivest and Adi Shamir^[4]. Our proposed schemes have the same roles as the ring signature, but our scheme needn't construct a ring. In our schemes, any signer can produce the signature entirely by himself using only his secret key and the others' identities. In particular, the other signers may be unaware that their identities have been involved into a signature.

Our proposed analogous ring signature schemes provide anonymity of the signer, thus making it impossible to determine who among the possible signers is the actual one.

The organization of this paper is as follows: In Section 2 we give the first analogous ring signature schemes, and the second proposed scheme in Section 3, and give an analysis of security to these signature schemes in Section 4. We make a concluding remark in the final section.

2 The first proposed signature schemes

In this section, we discuss the first proposed ID-based analogous ring signature scheme. The scheme consists of three participants: a key generation center for generating the secret key of all signers, a signer for producing anonymous signatures and a verifier for verifying signatures.

2.1 Notation

p_1, p_2 : are two safe large primes respectively and let n be $n = p_1 p_2$;

$g: g \in Z_n^*$ and the order is q ;

$\phi(n)$: is Euler function;

e : is a public exponent and satisfies $\gcd(\phi(n), e) = 1$;

ID_i : is the identity of signer U_i ($i = 1, \dots, k$) and satisfies $ID_i \in Z_n$;

$h(\cdot)$: a collision-resistant hash function and $\{0, 1\}^* \xrightarrow{*} \langle g \rangle$.

2.2 Signer's secret key generation

A Key Generation Center (KGC is an authentic authority) generates a secret key for signer U_i ($i = 1, \dots, k$). As for U_i , U_i 's secret key generation is as follows.

- (1) U_i sends own identity ID_i to KGC.
- (2) KGC computes $s_i^e = h(ID_i) \pmod{n}$ and sends s_i to U_i .
- (3) U_i checks $s_i \stackrel{?}{=} h(ID_i) \pmod{n}$.

2.3 Signature generation

Let $G = \{ID_1, ID_2, \dots, ID_k\}$ be a set of member's identities, then a member U_t with secret key s_t generates an anonymous signature to message m as follows.

- (0) Computes $y = h(ID_1 \parallel \dots \parallel ID_k)$.
- (1) $R = r^e \pmod{n}$, $c = s_t^{h(m \parallel R)} r \pmod{n}$, where r is a random number in Z_n .
- (2) $B = g^\alpha \pmod{n}$, where α is a random number in Z_n .
- (3) for $i = 1, \dots, k$, computes $C_i = h(ID_i)^{h(m \parallel R)} R \pmod{n}$.
- (4) w_1, w_2, \dots, w_k and $d_1, \dots, d_{t-1}, d_{t+1}, \dots, d_k$ are randomly chosen in Z_n^* .
- (5) Computes $T_t = y^{ew_t} \pmod{n}$ and for $j = 1, \dots, t-1, t+1, \dots, k$,

$$T_j = y^{ew_j} (B^e / C_j)^{d_j} \pmod{n}.$$
- (6) $d_t = d_0 - \sum_{j \neq t}^k d_j$ where $d_0 = h(T_1 \parallel \dots \parallel T_k \parallel h(m \parallel R) \parallel B)$.

(7) $r_t = w_t - d_t \alpha \pmod{q}$ and $r_j = w_j (1 \leq j \leq k, j \neq t)$.

the signer generates signature $(y, m, R, B, d_0, d_1, \dots, d_k, r_1, \dots, r_k)$.

2.4 Verification phase

We suppose that a receiver know all identities ID_i of members, the signature is verified as follows.

- (1) For $i=1, \dots, k$ compute $C_i = (h(ID_i))^{h(m \parallel R)} R \pmod{n}$.
- (2) confirm the equation $d_0 = \sum_{i=1}^k d_i \pmod{q}$.
- (3) for $(i=1, \dots, k)$ compute $T'_i = y^{\sigma_i} (B^e / C_i)^{d_i}$.
- (4) $d'_0 = h(T'_1 \parallel \dots \parallel T'_k \parallel h(m \parallel R) \parallel B)$.
- (5) check $d'_0 \stackrel{?}{=} d_0$, if the relation holds, then we accept the signature.

3 The second proposed signature schemes

The second signature parameter setup is the same as the above scheme. However, the signature size and computation of the second scheme are less than those of the first scheme.

The key generation center (KGC) produces private key $s_i = (ID_i)^{1/e}$ for each $U_i (1 \leq i \leq k)$. For member U_i , the signature of the signer U_i with ID_i is as follows.

- (1) chooses randomly $l \in Z_q$ and computes $y = s_i g^l \pmod{n}$.
- (2) the signer chooses a random number $w_i \in {}_R Z_q$ and computes $b_i = g^{w_i} \pmod{n}$.
- (3) For $j=1, \dots, t-1, t+1, \dots, k$,

The signer chooses $r_j, d_j \in {}_R Z_q$ and computes $b_j = g^{r_j} (y^e / ID_j)^{d_j}$.

- (4) the signer computes $c = h(b_1, \dots, b_k, m)$.
- (5) the signer computes $d_i = c - \sum_{j \neq i} d_j$ and $r_i = w_i - e d_i$.
- (6) the signer publishes signature $(d_1, r_1, \dots, d_k, r_k, m)$.

When the verifier receive the signature $(d_1, r_1, \dots, d_k, r_k, m)$. the checking process is as follows:

Checks $d_1 + d_2 + \dots + d_k \stackrel{?}{=} h(g^{r_i} (y^e / ID_1)^{d_1}, \dots, g^{r_k} (y^e / ID_k)^{d_k}, m)$.

4 Security Analysis

In this section, we give security analysis of the proposed schemes, because security analysis of the second signature is similar to one of the first scheme, we will only consider the first signature security analysis in the following section.

Theorem The first signature scheme is unconditional anonymity.

Proof Firstly, w_j, d_j of the first scheme (exception for d_i of the signer with ID_i) are chosen randomly, so that r_j is also random in Z_n . Secondly, r and each d_j or r_j have $n-1$ selections, the total selection of $(d_1, \dots, d_k, r_1, \dots, r_k, r)$ will be $(n-1)^{2k-1}$. Thirdly, any member of G can produce similar signature, any one cannot identify the identity of the signer from signature $(y, m, R, B, d_0, d_1, \dots, d_k, r_1, \dots, r_k)$. Furthermore, even if all secret keys are leaked, the attacker can't decide who signs the message. So that the scheme realizes unconditional anonymity.

Firstly, if the attacker wants to forge the signature of the signer U_i with ID_i . To forge a signature of the member U_i , the attacker must compute the e -th root of $h(ID_i)$, but he does not know the factor p_1 and p_2 , so that he can not compute the e -th root of $h(ID_i)$; and the attacker cannot generate a signature without secret member key of G .

Secondly, with a given signature $(y, m, R, B, d_0, d_1, \dots, d_k, r_1, \dots, r_k)$, the attacker can not forge a new signature. Although $d_1, \dots, d_k, r_1, \dots, r_k$ can be chosen randomly, it is as hard as to solve the difficulty of hash function for the attacker to choose $d_1, \dots, d_k, r_1, \dots, r_k$ satisfying the equation $d_0 = h(T_1 \parallel \dots \parallel T_k \parallel h(m \parallel R) \parallel B)$ and $d_0 = \sum_{i=1}^k d_i \pmod{q}$.

5 Unforgeability of the scheme

Proposition 1 The analogous ring signatures produced by the scheme proposed in Section 2 can be simulated in polynomial time, without knowing any of the secret keys of the ring, and with distribution of probability indistinguishable of ring signatures produced by legitimate signer, in the random oracle model.

Proof The simulation of the first ring signature scheme for a message m goes as follows.

- (0) randomly chooses a number y' in Z_n .
- (1) randomly selects r, s' in Z_n and computes $R = r^e \pmod{n}$, $c = s'^{h(m \parallel R)} r \pmod{n}$.
- (2) computes $B = cy'^\alpha \pmod{n}$, where α is a random number in Z_n .
- (3) for $i=1, \dots, k$, computes $C_i = h(ID_i)^{h(m \parallel R)} R \pmod{n}$.
- (4) w_1, w_2, \dots, w_k and $d_1, \dots, d_{t-1}, d_{t+1}, \dots, d_k$ are randomly chosen in Z_n^* .
- (5) Computes $T_t = y'^{aw_t} \pmod{n}$ and for $j=1, \dots, t-1, t+1, \dots, k$,

$$T_j = y'^{aw_j} (B^e / C_j)^d \pmod{n}.$$
- (6) $d_t = d_0 - \sum_{j \neq t}^k d_j$ where $d_0 = h(T_1 \parallel \dots \parallel T_k \parallel h(m \parallel R) \parallel B)$.
- (7) $r_t = w_t - d_t \alpha \pmod{q}$ and $r_j = w_j (1 \leq j \leq k, j \neq t)$.

If we assume $s'^e = h(ID_t) \pmod{n}$ then the signature $(y', m, R, B, d_0, d_1, \dots, d_k, r_1, \dots, r_k)$ is valid, but it is equivalent to solving the large number factorization problem to seek a number s' satisfying $s'^e = h(ID_t) \pmod{n}$.

6 Result

In this paper, we present two ID-based analogous ring signature schemes. The scheme makes any one cannot identify the actual identity of the signer from signature, even if one knows secret key of all members, he can't also distinguish which member sign message. Therefore, our proposed scheme realizes unconditional anonymity. An anonymous signature scheme has practical applications such as anonymous voting system, anonymous bid system and so on. With electronic commerce developing, the anonymous signature will play a more and more important role.

References

[1] Shamir A. Identity based cryptosystems and signature schemes. In: Proceedings of Crypto 84 on Advances in Cryptology. Springer-Verlag, 1985. 47 ~ 53

[2] Tseng Y, Jan Y. A novel ID-based group signature. In: Hwang TL, Lenstra AK eds. 1998 International Computer Symposium. Workshop on Cryptology and Information Security, Taiwan, 1998. 159~ 164

[3] Popescu C. Group signature schemes based on the difficulty of computation of approximate e -th roots. In: Proceedings of Protocols for Multimedia Systems (PROMS 2000). Poland, 2000. 325 ~ 331

[4] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: Boyd C, ed. Proc of Asiacrypt01, LNCS. Springer-Verlag, 2001. 2248; 552 ~ 565

两种基于 ID 的类环签名方案

张键红¹ 王继林² 王育民²

(1 北方工业大学理学院, 北京 100041; 2 西安电子科技大学 ISN 国家重点实验室, 西安 710071)

摘 要 给出了 2 种基于身份的类环签名方案, 在该方案中签名者能够代表他属于的集合, 但是, 验证者却不能识别哪个成员的签名. 对于一个攻击者而言, 即使他拥有所有成员的密钥, 他也不能决定是哪个成员签名, 从而实现了无条件的匿名性.

关键词 类环签名, 身份, 无条件的安全性