Information Sciences 179 (2009) 161–168

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

The ring authenticated encryption scheme – How to provide a clue wisely ☆

Jiqiang Lv [a,*], Kui Ren [b], Xiaofeng Chen [c], Kwangjo Kim [d]

[a] National Key Lab of ISN, Xidian University, No. 2, Taibai Road, Xi'an City, Shaanxi Province 710071, China
[b] Department of ECE, Illinois Institute of Technology, Chicago, IL, United States
[c] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China
[d] IRIS, Information and Communications University, 58-4 Hwaam-dong Yusong-ku, Taejon 305-732, Republic of Korea

ARTICLE INFO

Article history:
Received 17 July 2005
Received in revised form 30 July 2008
Accepted 5 September 2008

Keywords:
Public key cryptology
Ring signature
Authenticated encryption scheme

ABSTRACT

Though cryptography is being used more and more widely in reality, it seems that there exists no scheme or a concatenation of some existing schemes that could deal soundly with such practical situations as providing a clue, where the provider of the clue may want to reserve his beneficial rights while keeping his identity secret. To address this problem, inspired by the two notions of the ring signature and the authenticated encryption signature, we propose a new type of authenticated encryption scheme, which we call the ring authenticated encryption scheme, which can enable any member of a group of persons to provide a clue to some designated recipient wisely.

1. Introduction

Cryptography has been receiving extensive attention from both academia and industry during the past several decades, and a variety of digital signature schemes [9,18] have been proposed for use in different applications or situations in reality. However, there are still some practical applications that lack consideration, such as the issue of providing a clue; specifically, for example, a trusted police decides to arrest a criminal, but unfortunately it does not know any clue about the criminal's hiding place, except that it learns that a certain group of persons may know some. Thus, the police may encourage the members of this group to provide some clues, and promise to prize the person the police think who provides the most important clue. Finally, a member in this group, A_s say, wants to provide a clue, but he is not sure whether the clue to be provided could be the most important. Now he faces a problem: how to provide the clue wisely if he wants to use a digital scheme, where "wisely" means at least the following four requirements:

(1) Confidentiality of the clue – none except the designated police can get the clue. This requirement keeps another group member or an adversary from obtaining the clue and then sending it to the police after he intercepts the digital signature when transmitted in an insecure communication channel.
(2) Irretrievability of the provider's identity – none can retrieve the identity of the provider from the digital signature. This requirement guarantees that the provider can be protected if the clue is not the most important one; otherwise, he may suffer from being threatened. (A similar stronger requirement is unlinkability, which represents that none except the signer of the signature could determine whether two or more signatures are generated by the same signer).

☆ A conference version [12] of this paper was presented at *the 2004 Symposium on Cryptography and Information Security* (SCIS'04), JAPAN, January 2004.
* Corresponding author. Tel.: +86 029 88201015.
E-mail addresses: lvjiqiang@hotmail.com (J. Lv), kren@ece.iit.edu (K. Ren), isschxf@mail.sysu.edu.cn (X. Chen), kkj@icu.ac.kr (K. Kim).

0020-0255/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2008.09.014

(3) Verifiability of the provider's identity – if the clue is announced to be the most important by the police, the provider can prove without any disputation to the police or any third party that he is the real provider of the clue, which guarantees that he can get the prize.
(4) Unforgeability of the digital signature – the police or any third party cannot forge the digital signature.
If necessary, one more requirement:
(5) Undeniability – once a group member provides a valid digital signature on some clue, the police can prove to any third party that the signature is created by this group, and the group cannot repudiate this.

How could A_s achieve the above requirements? Obviously, more or less requirements above will not be met if A_s would adopt some currently existing digital signature, such as an encryption scheme, like that in [9], a conventional authenticated encryption scheme, like those in [10,11,21], a ring signature scheme, like those in [1,3,14,19], a group signature scheme, like that in [5] or other kind of digital schemes. To our knowledge, there exists no scheme or concatenation of some existing schemes that could solve the above issue soundly.

In this paper, inspired by the notions of the ring signature and the authenticated encryption scheme, we propose a new type of the authenticated encryption scheme, which we call the ring authenticated encryption scheme, which enables a member of a group of persons to provide a clue to a designated recipient wisely. By using our proposed ring authenticated encryption schemes, now A_s can provide the clue wisely. Only the designated police can obtain the clue by decrypting the valid ring authenticated encryption signature. If the clue is not the most important, A_s just keeps silent, and none can identify that he is the provider of the clue; if the clue is the most important, A_s can prove to the police (or any third party if necessary) that it is he who provides the clue, by showing some parameters that none else could generate. Any other group member who gets these secret parameters and claims that "I am the provider of the clue" will be easily spotted by the recipient (or the third party).

The remainder of the paper is organised as follows. In the next section, we briefly describe certain previous ring signature schemes and the authenticated encryption schemes. In Section 3, we give some necessary definitions. In Section 4, we propose two concrete ring authenticated encryption schemes, which can be used in two different situations, and discuss their security in Section 5. Section 6 concludes this paper.

2. Related works

In this section, we describe certain previously published ring signature schemes, and briefly review the notion of the authenticated encryption scheme.

2.1. Ring signatures

The concept of the ring signature is first introduced by Rivest et al. [19] in 2001, which is something like the group signature [5] but has the following special properties: (i) The ring signature has no group manager, and allows any group member to sign a message on behalf of the group without the cooperation of other group members; (ii) given a valid ring signature the recipient or a third party cannot tell which member of the group generates the signature; (iii) a group member can choose any sub-group belonging to the group, and if he is a member of the sub-group, he can sign a message on behalf of the sub-group without the content or assistance of the other members of the sub-group.

A few extensions of the ring signature have been proposed [1,3,13,14,16,23]. In 2002 Naor [16] proposed the concept of the deniable ring authentication scheme, building on the deniable authentication scheme and the ring signature. In January 2003, Lv et al. [13] proposed a discrete-logarithm based ring signature, building on the message-recovery signature scheme of Nyberg and Rueppel [17]. In September 2003, Lv and Wang [14] formalized the concept of the verifiable ring signature scheme, which has the additional property: if the signer of a signature is willing to disclose to the recipient or any third party that he generates the signature, then the recipient of the signature or the third party can correctly determine whether it is the case.

2.1.1. The ring signature scheme of Rivest et al.

Let (E_k, D_k) denote a pair of symmetric-key encryption and decryption algorithms using a key k, which we assume take as input an l-bit data block. Let $H(\cdot)$ denote a hash function whose hash values have the same length as the key of (E_k, D_k). Suppose that there are n persons in the group of possible signers, namely $A_0, A_1, \ldots, A_{n-1}$; and let $f_0, f_1, \ldots, f_{n-1} : \{0,1\}^l \to \{0,1\}^l$ be trap-door one-way functions, where the inverse f_i^{-1} of f_i can be computed only by the person A_i who knows the trap-door information of $f_i, (0 \leqslant i \leqslant n-1)$.

To generates a signature for a message M on behalf of the group, the signer A_s who can compute f_s^{-1} does the following.

Step 1. Select randomly a value c_0 from $\{0,1\}^l$, and compute $r_{n-1} = D_k(c_0)$, where $k = H(M)$.
Step 2. For $i = 0, 1, \ldots, s-1$, select randomly a value s_i from $\{0,1\}^l$, and compute $c_{i+1} = E_k(c_i \oplus f_i(s_i))$.
Step 3. For $i = n-1, n-2, \ldots, s+1$, select randomly a value s_i from $\{0,1\}^l$, and compute $r_{i-1} = D_k(r_i \oplus f_i(s_i))$.
Step 4. Compute $s_s = f_s^{-1}(c_s \oplus r_s)$ using the trap-door information of f_s. The signature on the message M is $(c_0, s_0, s_1, \ldots, s_{n-1})$.

A verifier first computes $k = H(M)$ and $c_{i+1} = E_k(c_i \oplus f_i(s_i))$, for $i = 0, 1, \ldots, n-1$. The signature is valid if and only if $c_n = c_0$ holds.

Rivest et al. [19] define a family of keyed combining functions $C_{k,\upsilon}(y_1, y_2, \ldots, y_r)$, which are still very useful in our following schemes. Every keyed combining function $C_{k,\upsilon}(y_1, y_2, \ldots, y_r)$ takes as input the key k, an initialization b-bit value υ, and arbitrary values $y_1, y_2, \ldots, y_r$. Given any fixed values for k and υ, each such combining function uses E_k as a sub-procedure, and outputs a b-bit value z, which has the following three properties:

(1) For each $s, 1 \leqslant s \leqslant r$, and for any fixed values of all the other inputs $y_i, i \neq s$, the function $C_{k,\upsilon}(y_1, y_2, \ldots, y_r)$ is a one-to-one mapping from y_s to the output z.
(2) For each $s, 1 \leqslant s \leqslant r$, given a value z and the values for all inputs y_i except y_s, it is possible to efficiently find a value y_s for such that $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) = z$.
(3) Given k, υ and z, it is infeasible for an adversary to solve the equation $C_{k,\upsilon}(g_1(x_1), g_2(x_2), \ldots, g_r(x_r)) = z$ for $x_1, x_2, \ldots, x_r$ if the adversary cannot invert any of the trap-door functions $g_1(\cdot), g_2(\cdot), \ldots, g_r(\cdot)$.

2.1.2. The discrete-logarithm based ring signature of Lv et al.

The discrete-logarithm based ring signature [13] consists of three phases: initialization, signature generation and signature verification.

Initialization: Each ring member, such as the ith member A_i, does follows,

Step 1. Choose two large primes p_i and q_i such that $q_i | p_i - 1$. Usually, p_i is longer than 512 bits, and q_i is longer than 160 bits. Let g_i be a generator of $GF(p_i)$ with order q_i.
Step 2. Choose $x_{A_i} \in Z_{q_i}$ as his private key, and compute the corresponding public key $y_{A_i} = g_i^{x_{A_i}} \bmod p_i$.
Step 3. Define a trap-door function $h_i(\alpha, \beta) = \alpha \cdot y_{A_i}^{\alpha \bmod q_i} \cdot g_i^{\beta} \bmod p_i$; and its inverse function $h_i^{-1}(y)$ is defined as $h_i^{-1}(y) = (\alpha, \beta)$, where α and β are computed as follows.

$$\alpha = y \cdot g_i^{-K} \bmod p_i, \tag{1}$$

$$\alpha^* = \alpha \bmod q_i, \tag{2}$$

$$\beta = (K - \alpha^*) \cdot x_{A_i}^{-1} \bmod q_i, \tag{3}$$

where K is a random integer in Z_{q_i}.

A_i makes p_i, q_i, g_i and y_{A_i} public, and keeps x_{A_i} secret.

Signature Generation: Suppose that the sth member A_s wants to sign a message M on behalf of r persons $A_1, A_2, \ldots, A_r$, where $1 \leqslant s \leqslant r$. A_s does the following.

Step 1. Compute the key k as $k = H(M)$.
Step 2. Pick uniformly and independently a pair of random values (α_i, β_i) for every other ring member $A_i, (1 \leqslant i \leqslant r, i \neq s)$, and compute $y_i = h_i(\alpha_i, \beta_i) \bmod p_i$.
Step 3. Pick randomly a b-bit initialization value υ, and solve out y_s from equation $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) = \upsilon$, where $C_{k,\upsilon}$ is the combining function defined in the ring signature scheme of Rivest et al.
Step 4. Compute $(\alpha_s, \beta_s) = h_s^{-1}(y_s)$ by using the trap-door information of h_s: First, choose a random integer $K \in Z_{q_i}$, compute α_s by Eq. (1), and keep K secret; second, compute α_s^* by Eq. (2); finally, computes β_s by Eq. (3).
Step 5. The ring signature σ on the message M is $(A_1, A_2, \ldots, A_r, \upsilon, (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_r, \beta_r))$.

Finally, A_s sends the message M and its signature σ to a recipient, *Bob* say.

Signature Verification: After receiving the ring signature σ, the recipient *Bob* does the following.

Step 1. Compute the key k as $k = H(M)$.
Step 2. Compute $y_i = h_i(\alpha_i, \beta_i) \bmod p_i$, for $i = 1, 2, \ldots, r$.
Step 3. Check $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) \stackrel{?}{=} \upsilon$. If it holds, then *Bob* accepts the signature as valid; otherwise, rejects it.

2.1.3. The verifiable ring signature of Lv and Wang

Building on Lv et al.'s discrete-logarithm based ring signature, Lv and Wang [14] formalized the concept of the verifiable ring signature scheme, which can enable the signer to prove to the recipient or a third party that the signature is really generated by him if he is willing to do so. The verifiable ring signature of Lv and Wang consists of four phases: initialization, signature generation, signature verification, and signer verification.

Initialization: The initialization phase is the same as that in the discrete-logarithm based ring signature of Lv et al. except the following two points:

(1) Each member A_i chooses another large prime o_i such that $o_i | q_i - 1$.
(2) The inverse $h_i^{-1}(y)$ of the trap-door function $h_i(\alpha, \beta)$ is defined as $h_i^{-1}(y) = (\alpha, \beta)$, where α and β are computed as follows.

$$\alpha = y \cdot g_i^{-K \cdot g_i^K} \bmod p_i, \tag{4}$$

$$\alpha^* = \alpha \bmod q_i, \tag{5}$$

$$\beta = x_{A_i} \cdot \alpha^* - K \cdot g_i^K \bmod q_i, \tag{6}$$

where K is a random integer that meets $K < o_i$.

The phases of signature generation and signature verification are the same as those in the discrete-logarithm based ring signature of Lv et al., except that (α_s, β_s) should be computed according to Eqs. (4)–(6).

Signer Verification: If the actual signer A_s is willing to prove to the recipient or a third party that the signature is generated by him, then the recipient can correctly determine whether it is the case by the following steps.

Step 1. A_s computes $S = g_s^K \bmod p_s$ and then sends S to the verifier.
Step 2. The verifier checks whether $y_s = \alpha_s \cdot S^S \bmod p_s$. Only if it holds could the verifier accept that the signature is really generated by A_s.

2.2. Authenticated encryption schemes

The concept of the authenticated encryption scheme is first introduced by Horster et al. [10] in 1994, which aims to achieve the purpose that the signature can only be verified by some designated recipients while the message is kept secret from the public. The authenticated encryption scheme requires a smaller communication bandwidth to achieve privacy, integrity and authentication of a message, when compared with the straightforward way that performs two separate processes on the message; firstly message encryption, and then message integrity and authentication.

However, in the authenticated encryption scheme of Horster et al., if the signer repudiates her signature later, there is no way for the recipient to prove the signer's dishonesty to any third party without disclosing his private key. To overcome this weakness, in 1999 Araki et al. [2] proposed an extended version of the authenticated encryption scheme, known as the convertible limited verifier scheme, which allows the recipient to convert an authenticated encryption signature to an ordinary signature so that a third party can verify its validity. But the recipient needs the cooperation of the signer when converting the signature, which is obviously a drawback under the situations that the signer refuses to cooperate. Therefore, a few new convertible authenticated encryption schemes [4,6,11,15,21,22] have been proposed where the recipient does not need the signer's cooperation when converting an authenticated encryption signature to an ordinary signature.

3. Definitions

We first give a definition of the ring authenticated encryption scheme, as follows.

Definition 1 (*Syntax*). A ring authenticated encryption scheme S^{RAE} consists of five polynomial-time algorithms: $(\mathscr{KG}^{RAE}, \mathscr{SG}^{RAE}, \mathscr{MRV}^{RAE}, \mathscr{SC}^{RAE}, \mathscr{SV}^{RAE})$:

$(sk, pk) \leftarrow \mathscr{KG}^{RAE}(1^l)$: A probabilistic algorithm that takes a security parameter l and outputs private key sk and public key pk. By using this algorithm, each member A_i generates his private key sk_i and the corresponding public key pk_i.
$\sigma \leftarrow \mathscr{SG}^{RAE}_{sk_s}(M, pk_b, g_s^{-1}, G)$: A probabilistic algorithm that takes the message M to be signed, the recipient *Bob*'s public key pk_b, the signer A_s's trap-door information of g_s^{-1} and any subset G of the other ring members' trap-door functions $\{g_1, g_2, \ldots, g_{s-1}, g_{s+1}, \ldots, g_n\}$, and outputs a ring authenticated encryption signature σ. (Note: $g_i$is public, where its inverse g_i^{-1} can be computed only by the ith ring member A_i who knows the trap-door information of g_i. These trap-door functions should satisfy some conditions, such as, when A_i computes g_i^{-1}, there should exist some secret parameter that can be used by A_i to prove to a recipient that the signature can only be created by him, without any information about A_i's secret disclosed.)
$(M, 1/0) \leftarrow \mathscr{MRV}^{RAE}_{sk_b}(\sigma)$: An algorithm that takes the signature σ and the recipient *Bob*'s private key sk_b, and outputs the message M and the (in)validity of the signature (where 1 means valid, and 0 means invalid). We require that $(M, 1) \leftarrow \mathscr{MRV}^{RAE}_{sk_b}(\mathscr{SG}^{RAE}_{sk_i}(M, pk_b, g_i^{-1}, G)$ for any message M, any subset G, any (sk_i, pk_i) generated using $\mathscr{KG}^{RAE}$.
$1/0 \leftarrow \mathscr{SC}^{RAE}(M, \Delta, \sigma)$: An algorithm that takes the signature σ, the message M and a parameter Δ that can only be recovered by the recipient *Bob* during executing the algorithm $\mathscr{MRV}^{RAE}_{sk_b}(\sigma)$, outputs whether the signature is really created by some ring member (where 1 means yes, and 0 means no). We require that $1 \leftarrow \mathscr{SC}^{RAE}(M, \Delta, \sigma)$ if *Bob* honestly executes the protocol $\mathscr{MRV}^{RAE}_{sk_b}(\sigma)$.
$1/0 \leftarrow \mathscr{SV}^{RAE}(\Theta)$: An algorithm that takes a parameter Θ created when A_s generates the signature σ, outputs whether A_s is the actual signer for the signature (where 1 means yes, and 0 means no). We require that Θ will not release any

information about the signer A_s's secret and that $1 \leftarrow \mathscr{SV}^{RAE}(\Theta)$ if σ is really generated by A_s. In addition, $\mathscr{P}^{RAE}$ should satisfy the condition that only the actual signer of the signature σ could provide such a parameter Θ that makes $1 \leftarrow \mathscr{SV}^{RAE}(\Theta)$.

Like a ring signature scheme, we require that a ring authenticated encryption scheme should also satisfy the property of signer ambiguity.

Definition 2 (*Signer Ambiguity*). Let G be a sub-group of a group of n persons $\{g_1, g_2, \ldots, g_n\}$, and suppose that $g_s \in G$ and each key is generated by $\mathscr{KG}^{RAE}(1^l)$. $\mathscr{SG}^{RAE}_{sk_s}(M, pk_b, g_s^{-1}, G \setminus \{g_s\})$ is perfectly signer-ambiguous if, for any message M, any G, any σ generated by $\mathscr{SG}^{RAE}_{sk_s}(M, pk_b, g_s^{-1}, G \setminus \{g_s\})$, given (G, M, σ), an adversary $\mathscr{A}$ outputs s such that $sk = sk_s$ with probability $1/|G|$.

The property of signer ambiguity says that it is infeasible for anyone except the signer of a signature to identity which member of the sub-group generates the signature.

4. Concrete ring authenticated encryption schemes

Under some practical situations, the recipient of a signature may hope that the third party who is verifying the signature explicitly knows that he is the designated recipient of the signature. However, under other situations the recipient may not hope so, but he may still hope that if he wants he can prove to the third party that he is the recipient. Therefore, when the recipient thinks that exposing that he is the designated recipient will benefit himself, he may go to prove that; otherwise, he may just keep silent.

In this section, we propose two ring authenticated encryption schemes that correspond to the above two different cases. Each of the proposed ring authenticated encryption schemes involves the following five phases: initialization, signature generation, message recovery and verification, signature conversion, and signer verification.

Before proceeding, we assume that there exist a family of keyed combining functions $C_{k,v}(y_1, y_2, \ldots, y_r)$ as described in Section 2.1, and a public one-way hash function $H(\cdot)$, which maps an input of arbitrary length to a bit string of constant length that can be used as key k for $C_{k,v}(y_1, y_2, \ldots, y_r)$.

4.1. Case 1: Explicit recipient

Initialization: Each member in a group,[1] such as the ith member A_i, chooses the following parameters: a large prime p_i such that it is hard to compute discrete logarithms in GF(p_i), another large prime q_i such that $q_i | p_i - 1$, a generator g_i in GF(p_i) with order q_i. Then, A_i chooses a random integer x_{A_i} from Z_{q_i} as his private key, and computes the corresponding public key $y_{A_i} = g_i^{x_{A_i}} \bmod p_i$. He defines a trap-door function $f_i(\alpha, \beta) = \alpha \cdot y_{A_i}^{\alpha \bmod q_i} \cdot g_i^{\beta} \bmod p_i$, and its inverse $f_i^{-1}(y)$ is defined as $f_i^{-1}(y) = (\alpha, \beta)$, where α and β are computed as follows.

$$\alpha = y \cdot g_i^{-K \cdot (g_i^K \bmod p_i) \bmod q_i} \bmod p_i, \tag{7}$$

$$\alpha^* = \alpha \bmod q_i, \tag{8}$$

$$\beta = K \cdot (g_i^K \bmod p_i) - x_{A_i} \cdot \alpha^* \bmod q_i, \tag{9}$$

where K is a randomly chosen integer from Z_{q_i}.

Finally, A_i publishes (y_{A_i}, p_i, q_i, g_i), and keeps x_{A_i} secret.

The recipient *Bob* chooses a large prime p such that it is hard to compute discrete logarithms in GF(p), another large prime q such that $q | p - 1$, a generator g in GF(p) with order q, and a random integer x_b from Z_q as his private key, computes his public key $y_b = g^{x_b} \bmod p$, and publishes (y_b, p, q, g).

Signature Generation: Suppose that the sth member A_s wants to sign a message $M (\in Z_p)$ to the recipient *Bob* on behalf of r ring members $A_1, A_2, \ldots, A_r$. Then, A_s does the following.

Step 1. Choose a random integer x from Z_q^*, compute

$$R = g^x \bmod p,$$
$$S = y_b^x \bmod p \bmod q,$$
$$V = M \cdot g^{-S} \bmod p,$$

and compute the key k as $k = H(M, S, V, y_b)$.

Step 2. Pick uniformly and independently a pair of random values (α_i, β_i) for every other ring member $A_i, (1 \leqslant i \leqslant r, i \neq s)$, and compute $y_i = f_i(\alpha_i, \beta_i) \bmod p_i$.

[1] The group will be called as the ring group in the following, and each member in the group will be called as a ring member.

Step 3. Pick randomly an initialization value υ, and solve out y_s from the equation $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) = \upsilon$.
Step 4. Compute $(\alpha_s, \beta_s) = f_s^{-1}(y_s)$ by using the trap-door information of f_s:
- First, choose a random integer K from Z_{q_s}, compute α_s by Eq. (7), and keep K secret;
- Second, compute α_s^* by Eq. (8);
- Finally, compute β_s by Eq. (9).

Step 5. The signature σ on the message M is

$$(A_1, A_2, \ldots, A_r, \upsilon, V, R, (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_r, \beta_r)).$$

Finally, the signer A_s sends σ to the recipient *Bob*.

Message Recovery and Verification: The recipient *Bob* does the following to recover and verify the message M from the signature σ.

Step 1. Compute $S = R^{x_b} \bmod p \bmod q$, recover the message $M = V \cdot g^S \bmod p$, and hash M, S, V and y_b to recover the key k as $k = H(M, S, V, y_b)$.
Step 2. Compute $y_i = f_i(\alpha_i, \beta_i) \bmod p_i$, for $i = 1, 2, \ldots, r$.
Step 3. Check $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) \stackrel{?}{=} \upsilon$. If it holds, then *Bob* accepts the signature as valid; otherwise, rejects it.

Signature Conversion: If the ring group repudiates its signature σ later, *Bob* can convert the signature to an ordinary signature such that any third party, *Alice* say, can verify whether the signature is generated by some ring member. Thus, *Bob* can prove the dishonesty of the ring group to any third party that. To achieve this, *Bob* does the following.

Step 1. *Bob* sends the message M, the parameter S and the signature component $(A_1, A_2, \ldots, A_r, \upsilon, V, (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_r, \beta_r))$ to *Alice*.
Step 2. *Alice* computes

$$k = H(M, S, V, y_b),$$
$$y_i = f_i(\alpha_i, \beta_i) \bmod p_i, \quad \text{for } i = 1, 2, \ldots, r.$$

Step 3. *Alice* checks $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) \stackrel{?}{=} \upsilon$. If it holds, then *Alice* believes that the signature is generated by some ring member; reject otherwise.

Signer Verification: If the actual signer A_s is willing to disclose to the recipient *Bob* (or any third party) that the signature is generated by him, then he does the following.

Step 1. A_s computes $X = g^K \bmod p_s$, and sends (X, y_{A_s}) to *Bob* ((X, y_{A_s}) and σ to the third party, respectively).
Step 2. *Bob* (the third party, respectively), who already knows (α_s, β_s), computes $\alpha_s^* = \alpha_s \bmod q_s$, and checks $X^X \stackrel{?}{=} g_s^{\beta_s} \cdot y_{A_s}^{\alpha_s^*} \bmod p_s$. Only the equation holds will *Bob* (the third party, respectively) accept that A_s is the real signer of the signature.

4.2. Case 2: Implicit recipient

During the three phases of signature generation, message recovery and verification, and signature conversion in the above scheme, if we replace the equation $k = H(M, S, V, y_b)$ with the new equation $k = H(M, S, V)$ and leave the remaining unchanged, then we can see that any verifier verifying the signature will not know who is the recipient of the signature. But the recipient *Bob* can prove to any third party, *Tom* say, that he is the recipient of the signature σ, as follows.

Recipient proof
Step 1. *Bob* sends the message M, the parameter S and the signature σ to *Tom*.
Step 2. *Tom* computes

$$k = H(M, S, V),$$
$$y_i = f_i(\alpha_i, \beta_i) \bmod p_i, \quad \text{for } i = 1, 2, \ldots, r.$$

Step 3. *Tom* checks $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) \stackrel{?}{=} \upsilon$. He continues if the equation holds; otherwise, terminate the protocol.
Step 4. In the following, *Bob* can prove to *Tom* that he knows $\log_R^S \bmod p\ (= x_b)$ by using a partial knowledge proof protocol as described in [7].

Note that if the recipient is unwilling to cooperate, then any third party cannot determine who is the real recipient, even though he gets the message M, the parameter S and the signature σ.

5. Security discussion

The security of proposed ring authenticated encryption schemes mainly relies on the following three assumptions.

Assumption 1 (*from [8]*). Suppose $H(\cdot)$ is a one-way hash function. It is computationally infeasible to derive x from a given hashed value $H(x)$, or to find two different values x, x^* such that $H(x) = H(x^*)$.

Assumption 2 (*from [19]*). Suppose $g_1(\cdot), g_2(\cdot), \ldots, g_r(\cdot)$ are a number of trap-door functions. Given two values υ and k, it is computationally infeasible to derive $x_1, x_2, \ldots, x_r$ without knowing the trap-door information of any of $g_1(x), g_2(x), \ldots, g_r(x)$, such that $C_{k,\upsilon}(g_1(x_1), g_2(x_2), \ldots, g_r(x_r)) = \upsilon$.

Assumption 3 (*from [20]*). For a given value $y \in Z_p$, it is computationally infeasible to derive x such that $y = g^x \bmod p$.

Correctness: (trivial)

Confidentiality: Obviously, only by using the private key x_b of the recipient could the message M and the parameter S be correctly recovered during the message recovery and verification phase. Furthermore, since an adversary cannot correctly compute the parameter S, nor could he represent it with his guessed message $\widehat{M}$ and the corresponding signature σ, thus, after the adversary gets the signature σ, he cannot determine whether his guessed message $\widehat{M}$ is the actual message by checking whether it satisfies those verification steps. Anyway, he can express the message $\overline{M}$ as $\overline{M} = V \cdot g^{\widehat{S}} \bmod p$ with a guessed $\widehat{S}$, and then determine whether it is the actual message by examining whether $k = H(\overline{M}, \widehat{S}, V, y_b)$ satisfies the verification equations. But the probability that the guessed $\widehat{S}$ happens to the actual S is $\frac{1}{q}$. Since q is a large prime, the probability is negligible.

Unforgeability: Anyone except the ring members cannot generate a valid signature during the signature generation phase, since it needs some ring member's private key to complete the signature. Assume an intruder intends to reveal the private key x_{A_s} from Eq. (9). Given a signature component (α_s, β_s), there is one more unknown parameter $K \cdot (g^K \bmod p_i) \bmod q_i$ in the above equation. Due to the intractability of the discrete-logarithm problem, the intruder cannot compute K from $X(= g^K \bmod p_i)$ that is used for the signer verification phase, so he cannot get the private key x_{A_s} of the signer from the equation. And every time the signer generates a signature, the parameter K should be different, so the number of secret parameters is always greater than the number of available equations. Therefore, the intruder cannot work out the private key successfully. Though a verifier could get $g^K \bmod p_s$ and (α_s, β_s) in the phase of signer verification, he cannot get the private key x_{A_s} from Eq. (9), for he cannot compute K from $g^K \bmod p_s$.

Any modification to the parameter V or R will make the inequality $k \neq H(M, S, V, y_b)$ (or $H(M, S, V)$) hold, therefore, the signature will not pass the following verification. Anyway, an adversary can randomly choose an integer $j, (1 \leqslant j \leqslant r)$, and a value υ, then he can choose all the (α_i, β_i) except (α_j, β_j). By the definition of trap-door functions, he can compute all the y_i, except y_j; He can solve out y_j from $C_{k,\upsilon}(y_1, y_2, \ldots, y_r) = \upsilon$. However, because he does not know the private keys x_{A_j}, so he will face the discrete logarithm problem when he solves (α_j, β_j) from the trap-door function $f_j(y_j)$. Even though, he can guess some pair (α_j^*, β_j^*), but the probability that the guessed pair satisfies the equation is $\frac{q_i}{p_i \cdot q_i} = \frac{1}{p_i}$. Since p_i is a large prime, the probability is also negligible.

It should be stressed that the signer, A_s, should choose different K every time he signs. Otherwise, if a verifier receives two identical $g^K \bmod p_i$ form two signatures generated by A_s, he can get the following two equations:

$$\begin{cases} K \cdot (g^K \bmod p_i) \bmod q_i = x_{A_s}\alpha_1^* + \beta_1 \bmod q_i \\ K \cdot (g^K \bmod p_i) \bmod q_i = x_{A_s}\alpha_2^* + \beta_2 \bmod q_i. \end{cases}$$

Finally, the verifier can solve out A_s's private key x_{A_s} as $x_{A_s} = (\beta_1 - \beta_2)(\alpha_2^* - \alpha_1^*)^{-1} \bmod q_i$.

Verifiability: If an adversary wants to impersonate the actual signer A_s during the signer verification phase, he must face discrete-logarithm problem – solving out X that satisfies $X^X = g_i^{\beta_i} \cdot y_{A_i}^{\alpha_i^*} \bmod p_i$ for some i.

Undeniability: Since only a ring member can generate a valid signature, so the recipient can determine whether a signature is valid. If the ring group repudiates its signature later, then by revealing the converted signature, the recipient can prove the dishonesty of the ring group to any third party. Therefore the ring group cannot repudiate its signature creation against anyone.

6. Conclusion

Building on the notions of the ring signature and the authenticated encryption signature, we propose the ring authenticated encryption scheme, which can enable any member of a group of possible signers to provide a clue wisely to some designated recipient. The ring authenticated encryption scheme has many important applications in reality.

Acknowledgements

The authors thank the anonymous referees for their helpful comments. The third author as well as his work is supported by National Natural Science Foundation of China (No. 60503006).

References

[1] M. Abe, M. Ohkubo, K. Suzuki, 1-out-of-*n* signatures from a variety of keys, in: Y. Zheng (Ed.), Advances in Cryptology – ASIACRYPT'02, LNCS, vol. 2501, Springer-Verlag, 2002, pp. 397–414.
[2] S. Araki, S. Uehara, K. Imamura, The limited verifier signature and its application, IEICE Transactions on Fundamentals E82-A (1) (1999) 63–68.
[3] E. Bresson, J. Stern, M. Szydlo, Threshold ring signature and application to ad-hoc groups, in: M. Yung (Ed.), Advances in Cryptology – CRYPTO'02, LNCS, vol. 2442, Springer-Verlag, 2002, pp. 465–480.
[4] T.Y. Chang, A convertible multi-authenticated encryption scheme for group communications, Information Sciences 178 (17) (2008) 3426–3434.
[5] D. Chaum, E.V. Heyst, Group signatures, in: D.W. Davies (Ed.), Advances in Cryptology – EUROCRYPT'91, LNCS, vol. 547, Springer-Verlag, 1991, pp. 257–265.
[6] H. Chien, Convertible authenticated encryption scheme without using conventional one-way function, Journal of Informatica 14 (4) (2003) 445–454.
[7] R. Cramer, I. Damgard, B. Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols, in: Y. Desmedt (Ed.), Advances in Cryptology – CRYPTO'94, LNCS, vol. 849, Springer-Verlag, 1994, pp. 174–187.
[8] W. Diffle, M. Hellman, New directions in cryptology, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.
[9] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory IT-31 (1985) 469–472.
[10] P. Horster, M. Michels, H. Petersen, Authenticated encryption schemes with low communication costs, IEE Electronics Letters 30 (15) (1994) 1212–1213.
[11] H. Huang, C. Chang, An efficient convertible authenticated encryption scheme and its variant, in: S. Qing, D. Gollmann, J. Zhou (Eds.), Proceedings of the Fifth International Conference on Information and Communications Security (ICICS'03), LNCS, vol. 2836, Springer-Verlag, 2003, pp. 382–392.
[12] J. Lv, K. Ren, X. Chen, K. Kim, Ring authenticated encryption: a new type of authenticated encryption, in: Proceedings of the 2004 Symposium on Cryptology and Information Security (SCIS'04), 2004, pp. 1179–1184.
[13] J. Lv, W. Xu, H. Zhang, X. Wang, A discrete-log based ring signature scheme (in Chinese), in: Proceedings of the First (China) National Symposium on Information and Networks Security, 2003, pp. 581–585.
[14] J. Lv, X. Wang, Verifiable ring signature, in: Proceedings of the Third International Workshop on Cryptology and Network Security (CANS'03), DMS Proceedings, 2003, pp. 663–665.
[15] J. Lv, X. Wang, K. Kim, Practical convertible authenticated encryption schemes using self-certified public keys, Applied Mathematics and Computation 169 (2) (2005) 1285–1297.
[16] M. Naor, Deniable ring authentication, in: M. Yung (Ed.), Advances in Cryptology – CRYPTO'02, LNCS, vol. 2442, Springer-Verlag, 2002, pp. 481–498.
[17] K. Nyberg, R.A. Rueppel, Message recover for signature schemes based on the discrete logarithm problem, in: A.D. Santis (Ed.), Advance in Cryptology – EUROCRYPT'94, LNCS, vol. 950, Springer-Verlag, 1995, pp. 182–193.
[18] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.
[19] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: C. Boyd (Ed.), Advances in Cryptology – ASIACRYPT'01, LNCS, vol. 2248, Springer-Verlag, 2001, pp. 257–265.
[20] B. Schneier, Applied Cryptology, second ed., Wiley, New York, 1996.
[21] T.S. Wu, C.L. Hsu, Convertible authenticated encryption scheme, The Journal of Systems and Software 62 (2002) 205–209.
[22] T.S. Wu, C.L. Hsu, K.Y. Tsai, H.Y. Lin, T.C. Wu, Convertible multi-authenticated encryption scheme, Information Sciences 178 (1) (2008) 256–263.
[23] F. Zhang, K. Kim, ID-based blind signature and ring signature from pairings, in: Y. Zheng (Ed.), Advances in Cryptology – ASIACRYPT'02, LNCS, vol. 2501, Springer-Verlag, 2002, pp. 533–547.