SCIS 2004 The 2004 Symposium on Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics, Information and Communication Engineers

Ring Authenticated Encryption: A New Type of Authenticated Encryption

Jiqiang Lv * Kui Ren * Xiaofeng Chen * Kwangjo Kim *

Abstract— By combining the two notations of ring signature and authenticated encryption together, we introduce a new type of authenticated encryption signature, called ring authenticated encryption, which has the following properties: signer-ambiguity, signer-verifiability, recipient-designation, semantic-security, verification-convertibility, verification-dependence and recipient-ambiguity. We also give a variant that does not hold the property of recipient-ambiguity but can make a verifier know to whom a signature is sent when he checks its validity.

Keywords: Public key cryptology; Authenticated encryption scheme; Ring signature

1 Introduction

Horster *et al.* [7] first proposed an authenticated encryption scheme modified from Nyberg-Ruepple's message signature [12], which aimed to achieve the purpose that the signature can only be verified by some specified recipients while keeping the message secret from the public. Compared with the straightforward approach employing the encryption and the signature schemes for a message, respectively, authenticated schemes require smaller bandwidth of communications to achieve privacy, integrity and anthentication of information. However, Horster *et al.*'s authenticated encryption scheme has a weakness that no one except the specified recipient can be convinced of the signer's signature, so it cannot make the recipient prove the dishonesty of the signer to any verifier without releasing his secret if the signer wants to repudiate his signature. To protect the recipient in case that the signer would repudiate his signature, Araki *et al.* [2] proposed a convertible limited verifier scheme to enable the recipient to convert the signature to an ordinary one so that any verifier can verify its validity. But it needs the cooperation of the signer when the recipient converts the signature, which is obviously a weakness under the situation that the signer is unwilling to cooperate. To overcome this weakness, Wu *et al.* [15] proposed another convertible authenticated encryption scheme. During which, the recipient can easily produce the ordinary signature without the cooperation of the signer, and he can reveal the converted signature and then any verifier can prove the dishonesty of the signer, if the signer wants to repudiate his signature. Recently, Huang *et al.* [8] showed that the scheme of Wu *et al.* does not consider that once an intruder knows the message then he can also easily convert a signature into an ordinary one, and they proposed a new convertible authenticated encryption scheme to overcome this weakness. However, we find that both these two schemes cannot provide semantic security for the message, since any adversary can determine whether his guessed message is the actual message signed by the original signer after he gets a valid signature. Semantic security is of very importance to an authenticated encryption scheme. Otherwise, if the message is too short, namely "yes" or "no", then obviously, an adversary can determine which message the signer signed by checking the verification equations.

Unlike group signature [4], ring signature, introduced by Rivest *et al.*[13], has the following special properties: Ring signature has no group managers, no setup procedures and no cooperation. A verifier cannot tell which member of a set of possible signers actually produced the signature; Any user can sign on behalf of any set to which he belongs, and he can choose a new set to each message without getting the content or assistance of the other members. Recently, some research has been done on ring signature [16, 3, 1]. From the Nyberg-Rueppel signature, J.Lv *et al.* proposed a DL-based ring signature [10] and modified it to a verifiable ring signature [9] which has the additional property: if the actual signer is willing to prove to a recipient that he actually signs the signature, then the recipient can correctly determine whether this is the fact. Based on the deniable authentication and Rivest *et al.*'s ring signature, Naor [11] proposed deniable ring authentication.

1.1 Our Results

In this paper, we combine the two notations of ring signature and authenticated encryption together and obtain a new type of authenticated encryption, called ring authenticated encryption. Ring authenticated encryption signature has some important applications in reality. For example, if a police wants to arrest a criminal but knows few clues about him, so it promises to give an award to a person in some group who could

* International Research center for Information Security (IRIS), Information and Communications University (ICU), 119 Munji-ro, Yusong-gu, Daejeon, 305-732, Republic of Korea (jiqiang,rkui,crazymount,kkj@icu.ac.kr)

provide the most important clue after the criminal is arrested. A group member may provide something, but he is not sure whether his message could be the most important one. To protect his message from propagating, he can first authenticatedly encrypt the message, and later prove to the police that he provides the most important clue if it is announced to be most important.

1.2 Organization

The rest of the paper is organized as follows. In the next section, we briefly describe the RSA-based ring signature of Rivest *et al.*. In Section 3, we define ring authenticated encryption scheme and present a DL-based concrete example. In Section 4, we give a variant that does not hold the property of recipient-ambiguity but can make a verifier know to whom a signature is sent when he checks its validity. In Section 5, we discuss the security and computational and communication complexity of the scheme. A conclusion will be given in Section 6.

2 RSA-Based Ring Signatures of Rivest *et al.*

Let $f_i : \{0,1\}^l \to \{0,1\}^l$ be a trapdoor one-way permutation where its inverse, f_i^{-1}, can be computed only if the trapdoor information is known. Let E and D be a symmetric-key encryption and decryption function whose message space is $\{0,1\}^l$, respectively. Let $H(\cdot)$ be a hash function whose output domain matches to the key-space of E and D.

Given $f_0, f_1, \cdots, f_{n-1}$, the signer who can compute f_s^{-1}, generates a signature for message M in the following way,

Initialization Randomly select c_0 from $\{0,1\}^l$ and computes $r_{n-1} = D_k(c_0)$, where $k = H(M)$;

Forward Sequence For $i = 0, 1, \cdots, s-1$, randomly select s_i from $\{0,1\}^l$ and compute $c_{i+1} = E_k(c_i \oplus f_i(s_i))$;

Backward Sequence For $i = n-1, n-2, \cdots, s+1$, randomly select s_i from $\{0,1\}^l$ and compute $r_{i-1} = D_k(r_i \oplus f_i(s_i))$;

Shaping Into A Ring Compute $s_s = f_s^{-1}(c_s \oplus r_s)$. The resulting signature is $(c_0, s_0, s_1, \cdots, s_{n-1})$.

A signature is valid if $c_n = c_0$ holds after computing $k = H(M)$ and $c_{i+1} = E_k(c_i \oplus f_i(s_i))$, for $i = 0, 1, \cdots, n-1$.

During the above scheme, Rivest *et al.* define a family of keyed combining functions $C_{k,v}(y_1, y_2, \cdots, y_r)$, which are still very useful in our scheme. Every keyed combining function $C_{k,v}(y_1, y_2, \cdots, y_r)$ takes as input a key k, an initialization value v, and arbitrary values $y_1, y_2, \cdots, y_r$ in $\{0,1\}^b$. Given any fixed values for k and v, each such combining function uses E_k as a subprocedure, and produces as output a value z in $\{0,1\}^b$. Each such combining function has the following three properties,

1. *Permutation on each input*: For each $s, 1 \le s \le r$, and for any fixed values of all the other inputs $y_i, i \ne s$, the function $C_{k,v}(y_1, y_2, \cdots, y_r)$ is a one-to-one mapping from y_s to the output z.

2. *Efficiently solvable for any single input*: For each $s, 1 \le s \le r$, given a b-bit value z and values for all inputs y_i except y_s, it is possible to efficiently find a b-bit value y_s for such that $C_{k,v}(y_1, y_2, \cdots, y_r) = z$.

3. *Infeasible to solve verification equation for all inputs without trapdoors*: Given k, v and z, it is infeasible for an adversary to solve the equation $C_{k,v}(g_1(x_1), g_2(x_2), \cdots, g_r(x_r)) = z$, for $x_1, x_2, \cdots, x_r$, if the adversary cannot invert any of the trap-door functions $g_1(x), g_2(x), \cdots, g_r(x)$.

3 Proposed Ring Authenticated Encryption

3.1 Definition and Requirements

Let $g_i (i = 1, 2, \cdots, r) : \{0,1\}^l \to \{0,1\}^*$ be a public trapdoor one-way permutation, where its inverse, g_i^{-1}, can only be computed by the i-th ring member A_i who knows the trapdoor information; These trapdoor functions should satisfy some conditions, such as, when A_i computes g_i^{-1}, there should be some secret parameter that can be used later to prove to a recipient that the signature is created by A_i, without releasing any information about A_i's secret key.

Definition 1 *Our ring authenticated encryption scheme, $S^{1,n}$, is a tuple of polynomial-time algorithms, $S^{1,n} = (G^{1,n}, E^{1,n}, V^{1,n}, C^{1,n}, R^{1,n}, S^{1,n})$,*

$(sk, pk) \leftarrow G^{1,n}(1^k)$: A probabilistic algorithm that takes security parameter k and outputs private key sk and public key pk.

$\sigma \leftarrow E^{1,n}(M, pk_b, g_s^{-1}, g_1, g_2, \cdots, g_{s-1}, g_{s+1}, \cdots, g_r)$: A probabilistic algorithm that takes message M, the recipient Bob*'s public key pk_b, the signer A_s's reverse trapdoor function g_s^{-1} and all the other ring members' trapdoor functions $g_i, i = 1, 2, \cdots, r, i \ne s$, outputs a ring authenticated encryption signature σ.*

$M, 1/0 \leftarrow V^{1,n}(sk_b, \sigma)$: An algorithm that takes the signature σ and the recipient Bob*'s secret key sk_b, outputs the authenticated message M and return 1 or 0 meaning accept or reject the information that the signature is created by some ring member, respectively. We require that $M, 1 \leftarrow V^{1,n}(sk_b, E^{1,n}(M, pk_b, sk_s, g_1, g_2, \cdots, g_{s-1}, g_{s+1}, \cdots, g_r))$ for any message M, any (sk_i, pk_i) generated by $G^{1,n}$.*

$1/0 \leftarrow C^{1,n}(M, \Delta, \sigma)$: An algorithm that takes the signature σ, the message M and a parameter Δ that can only be computed by the recipient Bob*, outputs 1 or 0 meaning accept or reject the information that the signature is really created by some ring member, respectively. We require that $1 \leftarrow C^{1,n}(M, \Delta, \sigma)$ if* Bob *does the protocol $V^{1,n}$ honestly.*

$1/0 \leftarrow R^{1,n}(M, \sigma, \Delta, t)$: An algorithm that takes the signature σ, the message M, the parameter Δ released by Bob *and a secret parameter t randomly selected by a verifier, outputs 1 or 0 meaning accept or reject the information that the signature is really sent to* Bob*. We require that $1 \leftarrow R^{1,n}(M, \sigma, \Delta, t)$ if* Bob *is the real recipient.*

$1/0 \leftarrow S^{1,n}(\Theta)$: An algorithm that takes a parameter Θ produced when A_s creates the signature σ, outputs 1

or 0 meaning accept or reject the information that A_s is the actual signer. We require that $1 \leftarrow S^{1,n}(\Theta)$ if Θ is really produced by A_s.

$S^{1,n}$ should satisfy the condition that only the actual signer could provide such a parameter that makes it equal 1 corresponding to a certain signature σ and that Θ will not release the signer's secret.

A ring authenticated encryption scheme has the following properties:

- *Signer-Ambiguity*: Anyone cannot determine which ring member creates an authenticated encryption signature if the actual signer is unwilling to expose himself;
- *Signer-Verifiability*: If the actual signer is willing to prove to a recipient that it is he who actually signs the signature, then the recipient can correctly determine whether it is the case;
- *Recipient-Designation*: Only the designated recipient could recover the message;
- *Semantic-Security*: Any adversary cannot determine whether his guessed message is the actual message signed by the original signer, even though he gets a valid signature;
- *Verification-Convertibility*: Anyone can verify, without the cooperation of any ring member, whether a signature is signed by some ring member, after the recipient reveals some parameters;
- *Verification-Dependence*: If the recipient does not reveal some parameter, any verifier cannot check the validity of the signature even though he gets the message and the corresponding signature;
- *Recipient-Ambiguity*: A verifier can not know to whom a signature is sent while verifying its validity. Only under the cooperation of the recipient could a verifier determine whether a signature is sent to the recipient.

3.2 A DL-Based Ring Authenticated Encryption Scheme

We assume the existence of a family of keyed combining functions $C_{k,v}(y_1, y_2, \cdots, y_r)$ and a publicly defined collision-resistant hash function $H(\cdot)$ that maps arbitrary inputs to strings of constant length, which are used as keys for $C_{k,v}(y_1, y_2, \cdots, y_r)$.

The ring authenticated encryption scheme consists of six phases: initialization, signature generation, message recovery and verification, conversion, recipient proof and signer verification.

Initialization

All the ring members cooperatively determine some common domain parameters: They first choose a large prime p such that it is hard to compute discrete logarithms in $GF(p)$, choose q such that q is a large prime divisor of $p-1$, choose o such that o is a large prime devisor of $q-1$, lets g be a base point of $GF(p)$ whose order is q; Publish p, q and g.

Then, each ring member, such as the i-th member A_i, chooses $x_{A_i}, (x_{A_i} < q)$ as his private key and computes the corresponding public key $y_{A_i} = g^{x_{A_i}} \bmod p$. He finally defines a trap-door function $g_i(\alpha, \beta)$ as $g_i(\alpha, \beta) = \alpha \cdot y_{A_i}^{\alpha^*} \cdot g^{\beta} \bmod p$, its inverse function $g_i^{-1}(y)$ is defined as $g_i^{-1}(y) = (\alpha, \beta)$, where

$$\alpha = y \cdot g^{-K \cdot g^K} \bmod p, \tag{1}$$

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

$$\beta = K \cdot g^K - x_{A_i} \cdot \alpha^* \bmod q, \tag{3}$$

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

A_i publishes y_{A_i} to all the other ring members, and keeps x_{A_i} secret.

Signature Generation

Step 1. To sign a message $M \in Z_p$, the signer, A_s say, who knows the public key $y_b (= g^{x_b} \bmod p)$ of the recipient *Bob*, whose corresponding secret key is x_b, randomly chooses two integers x_0 and x_1 from Z_q^*, computes

$$u_0 = M \cdot y_b^{q-x_0} \bmod p,$$
$$c_0 = g^{x_0} \bmod p,$$
$$u_1 = y_b^{x_1} \bmod p,$$
$$c_1 = g^{x_1} \bmod p,$$

then he computes the symmetric key k as $k = H(M, u_0, c_0, u_1)$.

Step 2. A_s picks an initialization value v uniformly at random from $\{0,1\}^b$;

Step 3. A_s picks random (α_i, β_i) for all the other ring members $A_i, (1 \leq i \leq r, i \neq s)$, uniformly and independently, and computes

$$y_i = g_i(\alpha_i, \beta_i) \bmod p.$$

Step 4. A_s solves the following equation for y_s:

$$C_{k,v}(y_1, y_2, \cdots, y_r) = v.$$

Step 5. A_s uses his knowledge of his trap-door function to obtain $(\alpha_s, \beta_s) = g_s^{-1}(y_s)$,

First, A_s chooses a random integer $K (< o)$, computes α_s by Eq.(1), and keeps K secret;

Second, computes α_s^* by Eq.(2);

Finally, computes β_s by Eq.(3).

Step 6. The signature σ on the message M is $(A_1, A_2, \cdots, A_r, v, u_0, c_0, c_1, (\alpha_1, \beta_1), (\alpha_2, \beta_2), \cdots, (\alpha_r, \beta_r))$.

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

Message Recovery and Verification

After receiving the signature σ, the recipient *Bob* does the following,

Step 1. *Bob* computes

$$u_1^* = c_1^{x_b} \bmod p,$$

$$M^* = u_0 \cdot c_0^{x_b} \bmod p,$$

and then he hashes the message M^*, the three parameters u_0, c_0 and u_1^* to compute the encryption key k:

$$k^* = H(M^*, u_0, c_0, u_1^*).$$

Step 2. For $i = 1, 2, \cdots, r$, *Bob* computes $y_i = g_i(\alpha_i, \beta_i) \bmod p$;

Step 3. *Bob* checks that whether $y_i, (i = 1, 2, \cdots, r)$ satisfy the fundamental equation:

$$C_{k^*,v}(y_1, y_2, \cdots, y_r) = v.$$

If the above equation holds, *Bob* accepts the signature as valid. Reject otherwise.

Conversion

If *Bob* wants to prove to any verifier, *Alice* say, that the signature is signed by some ring member, they can do as follows,

Step 1. *Bob* sends the message M^*, the parameter u_1^* and the signature σ to *Alice*.

Step 2. *Alice* computes $k = H(M^*, u_0, c_0, u_1^*)$, $y_i = g_i(\alpha_i, \beta_i) \bmod p$, for $i = 1, 2, \cdots, r$.

Step 3. *Alice* checks that whether $y_i, (i = 1, 2, \cdots, r)$ satisfy the fundamental equation:

$$C_{k,v}(y_1, y_2, \cdots, y_r) = v.$$

If the above equation holds, *Alice* convinces that the signature is signed by some ring member. Reject otherwise.

Recipient Proof

If *Bob* wants to prove to any verifier *Tom* that the signature σ is sent to him, they can do as follows:

Step 1: *Bob* first sends the message M^*, the parameter u_1^* and the signature σ to *Tom*.

Step 2. *Tom* computes $k = H(M^*, u_0, c_0, u_1^*)$, $y_i = g_i(\alpha_i, \beta_i) \bmod p$, for $i = 1, 2, \cdots, r$.

Step 3. *Tom* checks that whether $y_i, (i = 1, 2, \cdots, r)$ satisfy the fundamental equation:

$$C_{k,v}(y_1, y_2, \cdots, y_r) = v.$$

If it holds, he continues. Otherwise, terminate the protocol.

Step 4: *Tom* randomly selects an integer t from Z_q^*, and computes $X = c_1^t \bmod p$. Then he sends X to *Bob*.

Step 5: After receiving it, *Bob* computes $Y = X^{x_b} \bmod p$ and sends Y to *Tom*;

Step 6: *Tom* computes $u_1^{**} = Y^{t^{-1}} \bmod p$, and checks if $u_1^{**} = u_1^*$. Only if it holds does *Tom* accept that the signature is sent to *Bob*.

Signer Verification

If the actual signer, A_s, is willing to prove to the recipient *Bob* that he actually signs the signature, then he does the following,

Step 1. A_s computes $x = g^K \bmod q$, and sends (x, A_s) to *Bob*;

Step 2. *Bob* computes $\alpha_s^* = \alpha_s \bmod q$, and checks if x satisfies the following equalities:

$$\alpha_s \cdot x^x = y_s \bmod p.$$

$$x^x = g^{\beta_s} \cdot y_{A_s}^{\alpha_s^*} \bmod p,$$

If they hold, then *Bob* convinces that A_s is the real signer. Reject, otherwise.

4 Variant

During the signature generation protocol in our two schemes, if we replace the equation $k = H(M, u_0, c_0, u_1)$ with the new equation $k = H(M, u_0, c_0, u_1, y_b)$, and make some corresponding modifications during the left equalities that calculate the key k, then we can see that any verifier could verify whether a signature is sent to the recipient after the recipient releases the message M, the parameter u_1^* and the corresponding signature σ, instead of cooperation with him. The modified scheme has the same computation and communication costs as the original one, except that it does not hold the property that only under the cooperation of the recipient could a verifier determine whether a signature is sent to the recipient.

5 Analysis

5.1 Security

The security of our scheme is based on the following three assumptions:

Assumption 1 Intractability of reversing a one-way hash function*[6]: 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 Intractability of a keyed combining function*[13]: Given two values v and k, it is infeasible to derive $x_1, x_2, \cdots, x_r$ such that $C_{k,v}(g_1(x_1), g_2(x_2), \cdots, g_r(x_r)) = v$.*

Assumption 3 DL problem*[14]: For given $y \in Z_p$, it is computationally infeasible to derive x such that $y = g^x \bmod p$.*

During the signature generation protocol in the basic ring authenticated encryption scheme, an adversary can randomly choose an integer $j, (1 \leq j \leq r)$, and a b-bit value v, then he can choose all the (α_i, β_i) except (α_j, β_j). By the definition of trap-door functions, he can computes all the y_i, except y_j; He can compute y_j from $C_{k,v}(y_1, y_2, \cdots, y_r) = v$. Because he does not know the secret keys x_{A_j}, so he will face the DL problem when he solves (α_j, β_j) from the trap-door function $g_j(y_j)$. However, he can guess some pair (α_j^*, β_j^*), but the probability that the guessed pair satisfies the equation is $\frac{q}{p \cdot q} = \frac{1}{q}$. Since q is a large prime, the probability is negligible. Therefore, anyone except a ring member cannot generate a valid signature, since it needs the secret key to complete the signature. After an adversary gets the signature, he cannot guess the corresponding

message M, since he cannot correctly compute the parameter u_1 from c_1. Nor could he express the parameter u_1 with the his guessed message $\overline{M}$, c_1 or the corresponding signature σ. So our scheme provides semantic security of the message M. An adversary can obtain y_s and (α_s, β_s), but if he wants to solve the secret key x_{A_s} from Equ. (1),(2) and (3), he must again face the DL problem of solving $K \cdot g^K$ from $g^{K \cdot g^K}$. Any modification to the triple (u_0, c_0, c_1) will cause the inequality $k \neq H(M^*, u_0, c_0, u_1) \bmod p$ hold.

During the message recovery and verification protocol, only by using the secret key x_b of the recipient could the message M be correctly recovered. By the fact that only a ring member can generate a valid signature, the recipient can determine whether a signature is valid. From the steps in the scheme, we can draw the following theorem:

Theorem 1 *Given a message M's signature σ, following the steps in our basic ring authenticated encryption scheme, the recipient* Bob *will surely recover and verify the message M correctly from the signature.*

Proof: Since $g^q \bmod p = 1$, so *Bob* can get

$$\begin{aligned} & u_0 \cdot c_0^{x_b} \bmod p \\ = \; & M \cdot y_b^{q-x_0} \cdot (g^{x_0})^{x_b} \bmod p \\ = \; & M \cdot y_b^{q-x_0} \cdot y_b^{x_0} \bmod p \\ = \; & M \cdot y_b^q \bmod p \\ = \; & M. \end{aligned}$$

From the steps in signature generation, we know the theorem holds.

During the conversion protocol, if the recipient does not reveal the parameter u_1^*, any verifier cannot compute the key k, therefore cannot verify the validity of the signature, even he knows the the message M and the signature σ. After *Bob* reveals M, u_1^* and σ, any verifier can check its validity by following the steps in the scheme. Even after an adversary gets the two parameters u_1^* and c_1, he cannot compute *Bob*'s secret key x_b, which is a difficult DL problem. Once a ring member creates a valid signature, the recipient can always prove to any verifier that the signature is generated by some ring member.

During the recipient proof protocol, if the recipient is unwilling to cooperate with any verifier, then any verifier cannot determine who is the real recipient, even though he gets M, u_1^* and σ. From the steps in the scheme, we obviously have the following theorem,

Theorem 2 *The recipient* Bob *can prove to any verifier that the signature σ is sent to him by showing that he knows the parameter x_b with knowledge of a discrete logarithm between u_1^* and c_1.*

Proof:(sketch).

As for the security of signer verification, it is obviously a DL problem if a person wants to impersonate the actual signer. Though a verifier could get g^K, α and β in the process of signer verification, he cannot get the secret key x_{A_s} from Eq. (3), for he cannot compute $K \cdot g^K$ from g^K.

It should be stressed that the signer, A_s, should choose different random Ks every time when he signs. Otherwise, if a verifier receives two same g^K form two signatures signed by A_s, he can get the following two equations:

$$\begin{cases} K \cdot g^K = x_{A_s}\alpha_1^* + \beta_1 \bmod q \\ K \cdot g^K = x_{A_s}\alpha_2^* + \beta_2 \bmod q \end{cases}$$

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

From above, we can know our schemes meet the properties of strong unforgeability, strong undeniability, confidentiality, signer-verifiability, signer-ambiguity, recipient-designation, semantic-security, verification-convertibility, verification-dependence and recipient-ambiguity.

5.2 Computational and Communication Complexity

Let T_i denote the time for one inverse computation, T_e denote the time for one exponentiation computation, T_m denote the time for one modular multiplication computation, T_h denote the time for executing the adopted one-way hash function in each scheme, T_c denote the time for computing y_i from $C_{k,v}(y_1, y_2, \cdots, y_r) = v$, T_v denote the time for verifying whether $C_{k,v}(y_1, y_2, \cdots, y_r) = v$ holds for some given $k, y_1, y_2, \cdots, y_r$ and v, $|x|$ mean the bit length of an integer x.

Then in our ring authenticated encryption scheme: Length of original signature is $(r+3)|p| + r|q| + |b|$; Length of converted signature $(r+3)|p| + r|q| + |b|$; Computational complexity of signature generation is $(2r+4)T_e + (2r+2)T_m + T_h + T_i + T_c$; Computational complexity of message recovery is $T_e + T_m$; Computational complexity of message verifying is $(2r+1)T_e + 2rT_m + T_h + T_v$; Computational complexity of signature conversion is 0; Computational complexity of verifying converted signature is $2rT_e + 2rT_m + T_h + T_v$; Computational complexity of recipient proof conversion is $(2r+3)T_e + 2rT_m + T_h + T_v + T_i$; Computational complexity of signer verification is $T_e + T_m$.

6 Conclusion

By combining the two notations of ring signature and authenticated encryption together, we introduce a new type of authenticated encryption signature, called ring authenticated encryption, which has the following properties: signer-ambiguity, signer-verifiability, recipient-designation, semantic-Security, verification-convertibility, verification-dependence and recipient-ambiguity. We also give a variance that does not hold the property of recipient-ambiguity but can make a verifier know to whom a signature is sent when he checks its validity.

References

[1] M.Abe, M.Ohkubo and K.Suzuki, "1-out-of-n Signatures from a Variety of Keys". Advances

in Cryptology- ASIACRYPT2002, LNCS2501, pp.397-414. Springer-Verlag,2002.

[2] S.Araki, S.Uehara and K.Imamura, "The Limited Verifier Signature and Its Application". IEICE Transactions on Fundamentals, Vol. E82-A, No.1,pp.63-68,1999.

[3] E.Bresson, J.Stern and M.Szydlo, "Threhold ring signature and application to ad-hoc groups". Advances in Cryptology- CRYPTO2002, LNCS 2442, pp.465-480. Springer-Verlag, 2002.

[4] D.Chaum and E.V.Heyst,"Group Signatures" Advances in Cryptology- EUROCRYPT'91, LNCS 547, pp.257-265. Springer-Verlag,1991.

[5] R.Cramer, I.Damgard and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols". Advances in Cryptology- CRYPTO'94, LNCS 839,pp.174-187. Springer- Verlag,1994.

[6] W.Diffle and M.Hellman, "New Directions in Cryptology". IEEE Transactions on Information Theory,IT-22(6),pp.644-654,1996.

[7] P.Horster,M.Michels and H.Petersen, "Authenticated Encryption Schemes with Low Communication Costs". Electronics Letters, Vol. 30, No.15, pp.1212-1213,1994.

[8] H.Huang and C.Chang, "An Efficient Convertible Authenticated Encryption Scheme and its Variant", Proc. of ICICS2003-Fifth International Conference on Information and Communications Security, LNCS 2836, Springer-Verlag, pp.382-392, 2003.

[9] J.Lv and X.Wang, "Verifiable Ring Signature". Proc. of CANS03-International Workshop on Cryptology and Network Security, U.S.A, Sep.2003.

[10] J.Lv, W.Xu, H.Zhang and X.Wang, "DL-Based Ring Signature". First Workshop on Networks and Information Security, China, Jan.2003.

[11] M.Naor, "Deniable Ring Authentication". Advances in Cryptology-CRYPTO2002, LNCS 2442, pp.481-498, Springer-Verlag,2002.

[12] K. Nyberg and R.A.Rueppel, "Message Recover for Signature Schemes Based on the Discrete Logarithm Problem". Advance in Cryptology-EUROCRYPT94, LNCS 950, Springer-Verlag, pp.182-193,1995.

[13] R.L.Rivest,A.Shamir and Y.Tauman, "How to Leak a Secret". Advances in Cryptology- ASIACRYPT2001, LNCS 2248, pp.257-265, Springer-Verlag,2001.

[14] B.Schneier, Applied Cryptology, second edition,Wiley, New York, 1996.

[15] T.Wu and C.Hsu, "Convertible Authenticated Encryption Scheme". The Journal of Systems and Software, Vol. 62, pp.205-209, 2002.

[16] F.Zhang and K.Kim, "ID-Based Blind Signature and Ring Signature from Pairings". Advances in Cryptology- ASIACRYPT2002, LNCS 2501, pp.533-547, Springer- Verlag,2002.