Strong Designated Verifier Ring Signature Scheme

Ji-Seon Lee, Jik Hyun Chang
Dept. Computer Science, Sogang University,
1 Sinsu-dong, Mapo-gu, Seoul, Korea

Abstract-**In this paper, we propose a strong designated verifier ring signature scheme and discuss its security properties. The proposed scheme provides a way that leaks authoritative secrets to only a designated person anonymously by one of the group members and no one knows that the secret is from a group member or the recipient, except the recipient. This group is called a ring. We also propose a strong designated verifier ring signature with message recovery mechanism.**

Ⅰ. INTRODUCTION

In 2001, Rivest, Shamir, and Tauman [9] first formalized the concept of the ring signature. With a ring signature scheme, a signer can choose several members to form a temporary group called a ring and generate a ring signature without the assistance of the other ring members. Anyone can be convinced that the generated ring signature is from one of the ring members, but no one can identify the real signer among the ring members. This can be seen as a kind of non-interactive proof that a signer owns a witness of secret key that corresponds to one of *n* commitments of public keys. Subsequently, variant ring signature schemes have been proposed [1,2,3,4,5].

In 1996, Jakobsson, Sako, and Impagliazzo [6] introduced the concept of the designated verifier signature scheme which makes it possible for a signer to convince only the designated verifier that the signature is made by the signer. This is achieved since a designated verifier himself can efficiently simulate signatures that are indistinguishable from the signer's signature. Since the signer's public key and the designated verifier's public key are both included in the verification step, anyone can verify the signature. However, unlike ordinary digital signature schemes, no one can be convinced that who the real signer is, except the designated verifier. When the designated verifier Bob receives a signature from a signer Alice, he certainly trusts that it is from Alice upon verifying it, since he knows that he did not generate the signature himself. A designated verifier signature scheme is useful in some situations in which the signer should specify who may be convinced by the signer's signature. However, in some circumstances, the third party may be convinced with high probability that the signature intended for the designated verifier is actually generated by the signer. For example, the signature may be captured on the line by the third party before the designated verifier receives it. The third party can then confirm that the real signer is Alice. To protect the identity of the signer in such situations, the signer encrypts the signature with the designated verifier's public key so that only the designated verifier can get the signature generated by the signer with his secret key. This stronger requirement is called a strong designated verifier signature scheme and was discussed in [6]. Saeednia, Kremer, and Markowitch [10] proposed a new efficient designated verifier signature scheme which directly provides the strongness property without requiring any encryption of the signatures. In their scheme, the third party cannot even verify the signature since the secret key of the designated verifier is involved in the verification step. If the secret key of the designated verifier is exposed to the public, then anyone can verify the signature. However, still no one can confirm that the signature is from the signer or the designated verifier.

Rivest, Shamir, and Tauman [9] noticed that the designated verifier signatures can be implemented from ring signature scheme by including the verifier's public key in the ring. However, general ring signatures with simply involving the verifier's public key is not suitable to construct a strong designated verifier signature scheme.

Our Contribution: In this paper, we firstly propose a strong designated verifier ring signature scheme. Since the proposed scheme is a strong designated verifier signature, only the designated verifier can verify the signature and be convinced that the signature is made by one of the ring members. Since it is a ring signature, even the designated verifier does not have any idea who the real signer is among the *n* ring members. The proposed scheme would be useful in some situations. Suppose that someone wants to leak authoritative information only to a designated person or an institute in an anonymous way. He would sign that information which can be verified only by the designated recipient. The recipient knows that the information is from one of the ring members. However, except for the recipient, no one can tell from whom comes the information between a ring and a recipient since the recipient can simulate the signature in an indistinguishable way. As a variant of the proposed scheme, we also present a strong designated verifier ring signature scheme which prevents the third party from reading the message upon seeing the signature. We call this a strong designated verifier ring signature scheme with message recovery.

In section 2, we review Herranz and Saez's provably secure ring signature scheme. In section 3, we give some definitions of the proposed scheme and its security properties. In section 4, we propose our strong designated verifier ring signature and discuss its security properties. In section 5, we provide a strong designated verifier ring signature scheme which provides a message recovery mechanism. Some conclusions are made in section 6.

T. Sobh (ed.), Innovations and Advanced Techniques in Computer and Information Sciences and Engineering, 543–547.

Ⅱ. Herranz And Saez's Provably Secure Ring Signatures

Our scheme is based on Herranz and Saez's provably secure ring signature scheme [5]. In this section, we review their scheme.

Let p and q be two large primes such that $q \mid p-1$ and g be an element of $\mathbb{Z}_p$ of order q. The message to be signed is $m \in \mathbb{Z}_p$. We use (p, q, g) as common parameters to all n ring members and other participants in the scheme. Let H be a collision resistant hash function which outputs elements in $\mathbb{Z}_q$. Each member A_i, $1 \le i \le n$, has a private key $x_i \in \mathbb{Z}_q^*$ and the corresponding public key $y_i = g^{x_i} \bmod p$. Let L be a set of public keys of the ring members, that is, $L = \{y_1, ..., y_n\}$.

Signature Generation. To generate a ring signature for a message m on behalf of n ring members $A_1, ..., A_n$, a signer A_s, where $s \in \{1, ..., n\}$, follows the below steps.

(1) For all $i \in \{1, ..., n\}$, $i \neq s$, A_s randomly chooses $a_i \in \mathbb{Z}_q^*$ pairwise different and computes $R_i = g^{a_i} \bmod p$.

(2) A_s selects a random number $a \in \mathbb{Z}_q$.

(3) A_s computes $R_s = g^a \prod_{i \neq s} y_i^{-H(m, R_i)} \bmod p$. If $R_s = 1$ or $R_s = R_i$ for some $i \neq s$, then go to step (2).

(4) A_s computes $\sigma = a + \sum_{i \neq s} a_i + x_s H(m, R_s) \bmod q$.

(5) The signature is then $(L, m, R_1, ..., R_n, h_1, ..., h_n, \sigma)$, where $h_i = H(m, R_i)$, for all $1 \le i \le n$.

Signature Verification. The recipient checks that $h_i \stackrel{?}{=} H(m, R_i)$, for all $1 \le i \le n$. If this holds, the recipient verifies that the following equation holds or not.

$$g^{\sigma} = \prod_{1 \le i \le n} R_i \prod_{1 \le i \le n} y_i^{h_i} \bmod p$$

Herranz and Saez proved that their scheme satisfies anonymity and unforgeability in the random oracle model.

Ⅲ. Model

In this section, we define strong designated verifier ring signature scheme and its security properties.

Definition 1 A strong designated verifier ring signature scheme is defined by four procedures:

Key Generation Each member A_i, $1 \le i \le n$, in a ring has his key pair (x_i, y_i) and the designated verifier has his key pair (x_B, y_B).

Signature Generation If a user A_s, where $s \in \{1, ..., n\}$, wants to compute a strong designated verifier ring signature on behalf of a ring that includes himself, he executes signature generation algorithm with input a message m, the public key y_B of the designated verifier, the public key list L of the ring members and the signer's secret key x_s.

Signature Verification The designated verifier checks the validity of the signature. The output of this algorithm is true or false.

Transcript Simulation The designated verifier simulates transcripts that are indistinguishable from the signatures generated by any of the ring members.

The proposed strong designated verifier ring signature scheme should satisfy the following requirements:

- Signer Anonymity for the Designated Verifier : The designated verifier cannot determine the real signer among the n ring members with probability greater than $1/n$.

- Signer Anonymity for the Third Party (Strong Designated Verifier Property) : Any verifier cannot determine the real signer among the n ring members and a designated verifier with probability greater than $1/(n+1)$.

- Unforgeability : Any attacker must not succeed in forging a valid transcript for some message m on behalf of a ring or a designated verifier without the secret key of any ring members or the designated verifier.

Ⅳ. Strong Designated Verifier Ring Signatures

In this section, we propose a strong designated verifier ring signature scheme. We also provide security properties of the proposed scheme.

A. The proposed scheme

As in section Ⅱ, we use (p, q, g) as common parameters to all participants. Each member A_i, $1 \le i \le n$, has a key pair (x_i, y_i), the designated verifier Bob has his key pair (x_B, y_B), and $L = \{y_1, ..., y_n\}$.

Signature Generation. Among the n ring members, the signer A_s generates a strong designated verifier ring signature as follows :

(1) A_s randomly chooses $a_i \in \mathbb{Z}_q^*$ pairwise different and computes $R_i = g^{a_i} \bmod p$, for all $1 \le i \le n$, $i \neq s$.

(2) A_s chooses a random number $a \in \mathbb{Z}_q^*$.