A New Verifiable Ring Signature Scheme*

GAN Zhi, *CHEN Ke-fei*
(Department of Computer Science and Engineering,
Shanghai Jiatong University, Shanghai 200030, China)

Abstract: Ring signature is introduced by Rivest et al. In Rivest's scheme, even the actual signer of a ring signature cannot convince others about who is the actual signer. In this paper, we propose an efficient method to transform Rivest's scheme into a verifiable ring signature scheme. Then the actual signer can embed identification information in a so-called subliminal channel. If the actual signer is willing to prove to a verifier that it is him who actually signs the signature, then the verifier can correctly determine the actual signer among ring members.

Key words: ring signature; identification
CLC number: TP309 **Document code**: A **Article ID**: 0529-6579 (2004) S2-0132-03

1 Introduction

Ring signature is introduced by Rivest et al in [1], which has the following properties: the verifier can't tell which member of a set of possible signer actually produced the signature. Unlike group signature introduced in [2], ring signature has no group managers, no setup procedures and no cooperation. In addition to the properties of ring signature described above, it could be useful if the signer could prove that it is him who signs the signature. If a ring signature scheme has such property, we will call it verifiable ring signature scheme. Formally speaking, a verifiable ring signature scheme is a ring signature scheme which has three procedures:

(1) ring-sign $(m, P_1, P_2, \cdots, P_r, s, S_s)$ which produces a ring signature for the message, given the public keys $P_1, P_2, \cdots, P_r$ of the r ring members, together with the secret key S_s of the s-th member (who is the actual signer).

(2) ring-verify (m, σ) which accepts a message m and a signature σ (which includes the public keys of all the possible signers), and outputs either true or false.

(3) ring-check (σ) which is an interactive check process executed by a verifier so that the actual signer can pass the ring-check procedure and others will fail, both with an overwhelming probability.

In [3], Lu et al. proposed the first verifiable ring signature scheme. Their solution uses so-called double discrete logarithms which results in the complexity of signing to be rather high. Moreover, it needs that each ring member generates a special ring key pair, which is not a reasonable assumption in many cases. Instead, we found a method to transfer ring signature scheme of Rivest to a verifiable ring signature scheme. The only assumption of our scheme is that each member has a RSA public key.

2 Related Work

The ring signature scheme is useful for leaking secret. In [1] an appropriate example is given to illustrate the usage of ring signature: Suppose that Bob is a member of the cabinet of Utopia, and that Bob wishes to leak a juicy fact to a journalist about the escapades of the Prime Minister, in such a way that Bob remains anonymous, yet such that the journalist is convinced that the leak was indeed from a cabinet member.

As we can see, Bob cannot send to the journalist a standard digitally signed message. Since such a message, although it convinces the journalist that it came from a cabinet member, does so by directly revealing Bob's identity. A standard group signature scheme does not solve the problem, since it requires the prior cooperation of the other group members to set up, and leaves Bob vulnerable to later identification by the group manager, who may be controlled by the Prime Minister.

The correct approach is for Bob to send the story to the journalist signed with a ring signature scheme that names each cabinet member as a ring member.

Our scheme is based on Rivest's scheme. It can

* 收稿日期: 2004-08-23
基金项目: 国家自然科学基金资助项目
作者简介: 甘 志 (1977 年生), 男, 博士生; E-mail: gan-zhi@cs.sjtu.edu.cn

solve the problem of how to get rewards for leaking secret. After the Prime Minister was pull down, Bob can tell others it's him who so bravely revels the evil story of Prime Minister if he uses proposed scheme.

Then let's review ring signature due to Rivest. We assume that each member A_i has a RSA public key $P_i = (n_i, e_i)$ which specifies the trapdoor one-way permutation f_i of Z_n: $f_i(x) = x^{e_i} \pmod{n_i}$

We assume that only A_i knows how to compute the inverse permutation f_i^{-1} efficiently. E is a publicly defined symmetric encryption algorithm such that for any key k of length l, the function E_k is a permutation over b-bit strings. We define a combining function as follows:

$$C_{k,v}(y_1, y_2, \cdots, y_r) = E_k(y_r \oplus E_k(y_{r-1} \cdots \oplus E_k(y_1 \oplus v)))$$

Given a message to be signed, secret key S_s (the actual signer is the s-th member), and the sequence of public keys $P_1, P_2, \cdots, P_r$ of all the ring members, the signer computes a ring signature as follows:

(1) The signer computes the symmetric key k as the hash of the message m to be signed: $k = h(m)$, where h is a publicly defined collision-resistant hash function that maps arbitrary inputs to strings of length l.

(2) The signer picks an initialization value uniformly at random from $\{0,1\}^b$, where 2^b is larger than all the RSA module of ring members.

(3) The signer picks random x_i for all the other ring members, $1 \leqslant i \leqslant r, i \neq s$ uniformly and independently from, $\{0,1\}^b$, and computes $y_i = f_i(x_i)$.

(4) The signer solves the following ring equation for y_s: $C_{k,v}(y_1, y_2, \cdots, y_r) = v$.

(5) The signer uses his RSA private key to invert f_s on y_s to obtain.

(6) The signature of the message m is defined as $(P_1, P_2, \cdots, P_r; v; x_1, x_2, \cdots, x_r)$.

A verifier can verify an alleged signature $(P_1, P_2, \cdots, P_r; v; x_1, x_2, \cdots, x_r)$ on the message m as follows.

(7) First, for $i = 1, 2, \cdots, r$ the verifier computes $y_i = f_i(x_i)$.

(8) The verifier hashes the message to compute the encryption key $k = h(m)$.

(9) Finally, the verifier checks that the y_i's satisfy equation $C_{k,v}(y_1, y_2, \cdots, y_r) = v$. If it holds, the verifier accepts the signature as valid. Otherwise the verifier rejects.

In Rivest's ring signature scheme, the identity of the signer is unconditionally protected. After a ring signature is published, everybody including the actual signer can't give any evidence on who is the actual signer.

3 One-Time Scheme

In [3], Simmons invented the subliminal channel concept in conventional digital signature schemes. In any digital signature scheme, in which α bits are used to communicate a signature that provides β bits of security against forgery, where, $\alpha > \beta$, $\alpha - \beta$ bits are potentially available for subliminal communication. We notice that subliminal channel exists in ring signature scheme too. In a ring with n members, a signature consumes n random values: $v, x_i (i = 1, \cdots, n), i \neq s$). These random values compose a broadband subliminal channel. We will uses this subliminal channel to transfer signer's secret identification information.

For simplicity, we will embed secret information in so-called "glue value". Rivest et al. show "glue value" v can be obtained by always selecting 0 as v. In fact, we can set v to any value without hurt the security of the ring signature scheme. If we select some special v, then signer can prove that he is the actual signer among ring members.

At first, we propose an one-time identification scheme, which can be used to identification for only once. But this one-time scheme is very suitable for ring signature since there is no need to identify actual signer multiply times. To sign a message, the signer does the following:

(1) The signer chooses a random number r.

(2) The signer acts as the original scheme but let $v = h(h(r \| ID))$ where ID is identification information of signer.

After a signature is published, if the actual signer feels it's time to expose himself, he publishes $t = h(r, ID)$. Then everyone can verify his claim. If $v = h(t)$, then the actual signer will be correctly identified. Moreover, if the actual signer want to publish his identity, he may publish r and ID. Everyone should believe his claim if $v = h(h(r, ID))$ holds.

4 Zero-Knowledge Identification Scheme

One-time identification scheme is enough for many situations. But the signer may want to get rewards (for leaking secret) anonymously. Here we propose a zero-knowledge identification scheme. Bob can convince the verifier that he should give rewards to Bob without telling his identity to the verifier. The protocol is composed by two phases: information embedding phase and identification phase.

4.1 Information Embedding

To sign a message, the signer does the following:

(1) The signer acts as step 1 of original scheme.

(2) At first, signer selects two random prime number p and q, which make factoring $p \cdot q$ a ++ computational infeasible problem and $|p \cdot q| \leqslant b$. Signer then computes as $v = p \cdot q$.

(3) The signer acts as step 3, 4, 5, 6 of original scheme.

The above protocol embeds private information in the signature $(P_1, P_2, \cdots, P_r; v; x_1, x_2, \cdots, x_r)$. Then after the ring signature is published, signer can prove to a verifier that he is actual signer of this signature.

4.2 Identification Protocol

Signer can use several known zero-knowledge proofs for factoring to prove that he knows the factorization of v. We prefer the protocol proposed by Guillaume Poupard and Jacques Stern [5]. For a public integer n whose prime factors cannot be found by simple trial division, the protocol is a proof of knowledge of a small discrete logarithm of z'' mod n for a few randomly chosen elements z modulo n. The protocol is very efficient. When suitably optimized, its communication complexity is only $O(k + |n|)$ bits.

When the actual signer wants to execute the ring-check process, he proves to the verifier that he possesses the knowledge of the factorization of v through the interactive zero-knowledge proof protocol. Since only the actual signer knows the factorization of v, we know that the ring-check process is as secure as the zero-knowledge proof protocol.

5 Security Considerations

We have proposed a new verifiable ring signature scheme. The signer of the ring signature can prove to others that it is him who signs the message. Our scheme is almost the same as scheme of Rivest et al., except we embed signer's authentication information in initial "glue" value v, which won't affect the security of signature scheme. So our scheme as well satisfies the following properties: signer-ambiguity, unforgeability, confidentiality and non-repudiation.

6 Conclusion

In this paper, we proposed two verifiable ring signature schemes. The first is a one-time scheme. And the second is a zero-knowledge identification scheme. Both of the two schemes can satisfy the requirements of verifiable ring signature scheme. Now the actual signer can expose his identity whenever he wants to do so.

Although the first scheme is very simple, it's practical and very efficient. The second identification scheme is done through an interactive zero-knowledge proof for factoring problem. If the identification succeeds, the verifier knows that the prover is the actual signer. In both of the two schemes, the prover may choose if he should expose his identity.

References:

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [J]. Lecture Notes in Computer Science, 2001, 2248: 552—566.

[2] CHAUM D, van HEIJST E, PFITZMANN B. Cryptographically strong undeniable signatures, unconditionally secure for the signer (extended abstract) [J]. Lecture Notes in Computer Science, 1991, 576: 470—485.

[3] LU J Q, WANG X M. Verifiable ring signature [C]. In 2003 International Workshop on CRYPTOLOGY AND NETWORK SECURITY (CANS03), 2003.

[4] SIMMONS G J. The prisoner's channel and the subliminal channel [C]. In CRYPTO'83, 1984: 51—67.

[5] POUPARD G, STERN J. Short proofs of knowledge for factoring [C]. In PKC 2000, 2000: 147—166.

一个新的可验证环签名方案

甘 志, 陈克非

(上海交通大学计算机与工程系, 上海 200030)

摘 要: 在 Rivest 等提出的环签名方案中, 签名者可以隐藏自己的身份。即使存在一个拥有无穷计算能力的攻击者, 签名者的身份信息仍然是不可知的。在某些情况下, 环签名的实际签名者可能会希望证明签名人的身份, 然而 Rivest 的方案没有为签名者提供这种能力。提出了一种签名者可以揭示自己身份的环签名方案。签名者签发一个看似普通的环签名, 并在其具有的阈下信道中嵌入认证信息。随后, 一旦签名者出示其拥有的秘密信息, 那么任何人都可以正确的判断签名者的身份。

关键词: 环签名; 身份识别; 阈下信道

中图分类号: TP309