A Ring Signature Scheme Based on the Nyberg-Rueppel Signature Scheme

Chong-zhi Gao[1], Zheng-an Yao[2], and Lei Li[1]

[1] Institute of Software
Sun Yat-Sen University
Guangzhou 510275, China
[2] College of Mathematics and Computational Science
Sun Yat-Sen University
GuangZhou 510275, China

Abstract. Ring signature allows to specify a set of possible signers without revealing which member actually produced the signature. This concept was first formalized in 2001 by Rivest, Shamir, and Tauman[3]. Authors of [3] also proposed two versions of ring signature scheme. However, to achieve the goal of anonymity, each user should do much computation in the initial procedure: they should do much work to generate their private and public keys, e.g. in the RSA version, each user should find n_i such that it is the product of two distinct large prime and compute his private/public keys. Moreover, one should extend the one-way trapdoor functions to a common domain since these functions are computed in different domains. This paper's main contribution is to present a version of ring signature scheme which uses a common modulus. Thus, Our proposed scheme is much more efficient in the setup procedure. Further more, the size of public and private keys are reduced.

1 Introduction

Ring signature scheme was first formalized in 2001 by Rivest, Shamir, and Tauman[3]. A ring signature makes it possible to specify a set of possible signers without revealing which member actually produced the signature.

To achieve the goal of anonymity, each user should generate his public key and private key independently, i.e. there does not exist a trust center that do the initial work such as generating secret keys and transmitting these keys to users. For example, in the RSA version of the ring signature, each user should select n_i such that it is the product of two distinct large prime. Then he compute his public and private key. Obviously, this initial work involves much computation. Further more, it require the signer to do additional preparation when he generate the signature. Similarly, this happens in the Rabin version.

Nyberg and Rueppel [1,2] proposed a signature scheme based on the discrete logarithm problem. The Nyberg-Rueppel scheme allows signatures with message recovery. Our paper's main contribution is to present a ring signature scheme with a common modulus, i.e. all users compute in the domain $\mathbf{Z}_p$ where

J. Zhou, M. Yung, Y. Han (Eds.): ACNS 2003, LNCS 2846, pp. 169–175, 2003.

p is a large prime. Applying the Nyberg-Rueppel scheme to the ring signature, without weakening the security, different users need not do the computation in different domains. Thus, our proposed scheme is much more efficient in the setup procedure. Further more, the size of keys (public and private) are reduced.

1.1 Related Works

Chaum and van Heyst put forth the concept of a group signature scheme In 1991 ([4]). It allows a group member to sign messages anonymously on behalf of the group. However, the identity of the signature's originator can be revealed by the group manager if necessary. A group signature scheme could be used by an employee of a large company to sign documents on behalf of the company and it has further applications. Informal notions of ring signatures which was in the context of general group signatures can be finded in [4, 5]. However, the concept of ring signatures was first formalized in [3]. A threshold ring signature scheme was proposed in [6] by Emmanuel Bresson, Jacques Stern, and Michael Szydlo.

The rest of this paper is organized as follows. In section 2, we explain ring signatures and review some previous works. In section 3, we introduce our ring signature scheme and discuss its security and efficiency. In section 4, we conclude the paper.

2 Ring Signature

2.1 Ring Signature

The concept of ring signature was formalized by Rivest, Shamir, and Tauman in [3].

It is assumed that each possible signer is associated with a public key P_k that defined his signature scheme and specifies his verification key. The corresponding secret key (which is used to generate regular signature) is denoted by S_k. These possible signers are called a *ring*. It is also necessary that it is a trapdoor one-way function to generate and verify signatures.

A ring signature consists two procedures:

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

– 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*.

A ring signature scheme must satisfy the usual soundness and completeness condition. In addition the signatures should be *signer-ambiguous* : the verifier should be unable to determine the identity of the actual signer in a ring of size r with probability greater than $1/r$.

The scheme proposed in [3] has the property of unconditional anonymity in the sense that even an infinitely powerful adversary can not reveal the actual signer's identity.

2.2 Previous Work

To compare with our proposed method, we review the method in [3].

Combining Functions:

The concept of combining functions is very important in the ring signature scheme.

A Combing function $C_{k,v}(y_1, ..., y_r)$ takes as input a key k, an initialization value v, and arbitrary values $y_1, y_2, ..., y_r$ in $\{0,1\}^b$ such that given any fixed values for k and v, it has the following properties:

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

2. **Efficiently solvable for any single input:** For each s, $1 \leq s \leq r$, 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 for y_s such that $C_{k,v}(y_1, ..., y_r) = z$.

3. **Infeasible to solve verification equation for all inputs without trap-doors:** Given k, v and z, it is infeasible for an adversary to solve the equation

$$C_{k,v}(g_1(x_1), ..., g_r(x_r)) = z$$

for $x_1, x_2, ..., x_r$, (given access to each g_i, and to E_k) if the adversary can't invert any of the trap-door function $g_1, g_2, ..., g_r$.

[3] proposed a combining function:

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

where E_k is a symmetric encryption function which takes k as secret key.

It satisfies the three properties and the y_s is computed as follows:

$$y_s = E_k^{-1}(y_{s+1} \oplus ...E_k^{-1}(y_r \oplus E_k^{-1}(z))) \oplus E_k(y_{s-1} \oplus ...E_k(y_1 \oplus v)...)$$

Trap-Door Permutations and Extending Them to a Common Domain:

Each member $A_i (1 \leq i \leq r)$ generates his RSA key $k_i = (n_i, p_i, q_i, e_i, d_i)$. Where $P_i = (n_i, e_i)$ is his public key and $S_i = (p_i, q_i, d_i)$ is his private key.

The one-way permutation f_i of Z_{n_i} is defined as:

$$f_i(x) = x^{e_i} \pmod{n_i}$$

The inverse permutation f_i^{-1} is computed as:

$$f_i^{-1}(y) = y^{d_i} = x \pmod{n_i}.$$

However, the trap-door RSA permutations of the various ring members have domains of different sizes. The authors in [3] extend the permutations to have as their common domain the same set $\{0,1\}^b$, where 2^b is some power of two which is larger than all the modular n_i's.

The extended trap-door permutation g_i over $\{0,1\}^b$ is defined as:

For any b-bit input m define nonnegative integers t_i and r_i so that $m = t_i n_i + r_i$ and $0 \leq r_i < n_i$. Then

$$g_i(m) = \begin{cases} t_i n_i + f_i(r_i) & \text{if } (t_i+1)n_i \leq 2^b \\ m & else \end{cases}$$

For more details, please consult [3].

The Ring Signature of RSA Version in [3]:

Given the message m to be signed, the signer's secret key S_s, and the sequence of public keys $P_1, P_2, ..., P_r$ of all the ring members, the signer computes a ring signature as follows:

1. The signer computes $h(m)$ as the symmetric key k:

$$k = h(m)$$

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

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

$$y_i = g_i(x_i)$$

4. The signer solves the following ring equation for y_s:

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

By assumption, given arbitrary values for the other inputs, there is a unique value for y_s satisfying the equation, which can be computed efficiently.

5. The signer uses his knowledge of his trapdoor in order to invert g_s on y_s to obtain x_s:

$$x_s = g_s^{-1}(y_s).$$

6. The signature on the message m is defined to be the $(2r+1)$-tuple:

$$(P_1, P_2, ..., P_r; v; x_1, x_2, ..., x_r).$$

To verify a signature

$$(P_1, P_2, ..., P_r; v; x_1, x_2, ..., x_r)$$

on the message m, the verifier accepts the signature if and only if $C_{H(m),v}(f_1(x_1), f_2(x_2), ..., f_r(x_r))$ is equal to v.

3 Our Proposed Scheme – Nyberg-Rueppel Version

To achieve the goal of using common modulus when computing, we observe that the RSA signature scheme is not suitable for this goal. We also point out that general signature schemes is not suitable since it should be a trapdoor one-way function to generate and verify signatures. For example, the ElGamal signature scheme is not suitable. We should employ the signature schemes that anyone can generate "pseudo" signatures which can be successfully verified using the verification procedure. But only a person who has his secret key can generate a "real" signature of a message by his own choice.

Considering the Nyberg-Rueppel signature scheme, we find that it meet our requirement and thus can be applied to the ring signature scheme.

We build the trapdoor one-way functions based on the Nyberg-Rueppel signature scheme. Let's describe the ring signature scheme of Nyberg-Rueppel version in detail.

Combining Functions:
We use the same combining function proposed in [3], which was described in part 2.2 in our paper.

Trapdoor Functions using common modulus:
Let p be a prime such that the discrete log problem in $\mathbf{Z}_p$ is intractable. Let $\alpha \in GF(p)$ be an element of order q where q is equal to $p-1$ or is a large integer factor of $p-1$. (p, α) are the common parameters of all the ring members.

Each user A_i chooses his private key $S_i \in \mathbf{Z}_q$ and publishes his public key as $P_i = \alpha^{-S_i} \bmod p$.

The one-way function f_i takes a 2-tuple $(e, y) \in \mathbf{Z}_p \times \mathbf{Z}_q$ as input and output a single number in $\mathbf{Z}_p$. It is computed as follows:

$$f_i(e, y) = \alpha^y {P_i}^e e \bmod p$$

If one know the value S_i, one can find an inverse of x $(= f(e, y))$ by following steps:

First, randomly chooses $r \in \mathbf{Z}_p$, then computes:

$$e = x\alpha^{-r} \bmod p$$

$$y = r + S_i e \bmod q$$

and output (e, y).

This one-way function is derived from the Nyberg-Rueppel signature scheme. Note that there are not only one inverse of an x. Everyone can compute f_i using the public key P_i, but given $x \in GF(p), x \neq 0$, it is hard for anybody not in possession of S_i to compute an inverse of x, since it requires the solution of the equation:

$$x = \alpha^y {P_i}^e e \bmod p$$

for y and e. The security of Nyberg-Rueppel signature scheme was analyzed in [1] and [2].

The Ring Signature of Nyberg-Rueppel version:
If a signer who has the secret key S_s want to sign a message m, and the public keys of all the ring members are $P_1, P_2, ..., P_r$. The singer computes a ring signature as follows.

1. The signer computes $h(m)$ as the symmetric key k:

$$k = h(m)$$

2. The signer picks an initialization value v uniformly at random from $\{0,1\}^b$.
3. The signer picks random (e_i, y_i) uniformly and independently from $\mathbf{Z}_p \times \mathbf{Z}_q$ $(1 \leq i \leq r, i \neq s)$ and computes:

$$x_i = f_i(e_i, y_i)$$

4. The signer solves the following ring equation for x_s:

$$C_{k,v}(x_1, x_2, ..., x_r) = v$$

5. The signer uses his secret key S_i to invert f_s on x_s to obtain (e_s, y_s).
6. The signature on the message m is defined to be the $(2r+1)$-tuple:

$$(P_1, P_2, ..., P_r; v; (e_1, y_1), ..., (e_r, y_r))$$

To verify a signature

$$(P_1, P_2, ..., P_r; v; (e_1, y_1), ..., (e_r, y_r))$$

on the message m, the verifier accept the signature if and only if

$$C_{H(m),v}(f_1(e_1, y_1), f_2(e_2, y_2), ..., f_r(e_r, y_r))$$

is equal to v.

Security and Efficiency:

We use the combining function proposed in [3] and refer the reader to [3] for the analysis of the combining function's security. Now, Let's consider the one-way functions derived from Nyberg-Rueppel signature scheme. Everyone can compute f_i provided with the public key P_i. However, given the value of $f_i(e, y)$, only the one who has the secret key S_i can obtain (e_0, y_0) such that $f_i(e, y) = f_i(e_0, y_0)$. Hence, our proposed scheme satisfies the properties of completeness and soundness.

Our proposed scheme also has the property of unconditional anonymity, i.e. even an infinitely powerful adversary can not reveal the actual signer's identity, because given m and v, the function

$$C_{H(m),v}(f_1(e_1, y_1), f_2(e_2, y_2), ..., f_r(e_r, y_r))$$

has $p^{r-1}q^r$ solutions for $((e_1, y_1), (e_2, y_2), ..., (e_r, y_r))$. Every one of these solutions might be chosen with equal probability by an signer.

Let us take a look at the size of keys. The public key of each user is in $\mathbf{Z}_p$ and the private key is in $\mathbf{Z}_p$, whereas in the RSA version, the public key of user A_i is (n_i, e_i) in $\{0,1\}^b \times \{0,1\}^b$ and the private key is (p_i, q_i, d_i) in $\{0,1\}^{b/2} \times \{0,1\}^{b/2} \times \{0,1\}^b$ where $b/2$ is the approximate length of each prime in binary representation. Thus, the size of keys are greatly reduced.

Since the users need not to search large primes to compose their public keys and private keys, there is much less computation in the initial work. But our proposed scheme also has it's drawback: signing requires one modular exponentiation and two modular exponentiation for each non-signer; verification requires two modular exponentiation for each ring member. Thus, this scheme is more suitable in the case of small rings.

4 Conclusions

We have proposed a ring signature scheme using a common modulus. We showed that our method satisfies the property of unconditional anonymity and require much less computation in the setup procedure. Further more, the size of public and private keys are reduced.

References

[1] K. Nyberg and R. Rueppel, A new signature scheme based on the DSA giving message recovery, Proc. 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, Nov. 3–5., (1993), 4 pages.

[2] K. Nyberg and R. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem, in Advances in Cryptology-EuroCrypt'94, LNCS 950, pp.182–193, Springer-Verlag, 1995.

[3] R. Rivest, A. Shamir, and Y. Tauman, How to Leak a Secret, in Proc. Asiacrypt '01, pp. 552–565, Springer-Verlag, 2001.

[4] David Chaum and Eugène Van Heyst, Group signatures, in Advances in Cryptology Eurocrypt 91, pp. 257-C265, Springer Verlag, LNCS 547, 1991.

[5] Jan Camenisch, Efficient and generalized group signatures. In Walter Fumy, editor, Advances in Cryptology C Eurocrypt 97, pp. 465-C479, Springer Verlag, LNCS 1233, 1997.

[6] Emmanuel Bresson, Jacques Stern, Michael Szydlo, Threshold Ring Signatures for Ad-hoc Groups , in Advances in Cryptology – CRYPTO'2002, pp. 465-C480, Springer Verlag, LNCS 2442, 2002.