Abstract: We introduce a verifiable ring signature that not only has all the properties of a ring signature, but also the following property: if the actual signer is willing to prove to the verifier that he actually signs the signature, then the verifier can correctly determine whether he is the actual signer among the possible signers.

Keywords: Public-key cryptography, Digital signature, Ring signature

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 signers actually produced the signature; Unlike group signature introduced in [2], ring signature has no group managers, no setup procedures and no cooperation, that is, 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 [3,4,5,6]. [3] proposes an ID-based ring signature, [4] extends the ring signature in [1] to a threshold scheme and [5] considers a ring authentication scheme that accepts variety of public-keys and a threshold of signers.

In addition to the properties of ring signature described above, it could be useful if there were some secret information, though which the signer could prove that it is he who signs the signature if he was willing to do so later. We will call such signatures verifiable ring signatures. A verifiable ring signature can be used in some situations, such as when the police want to arrest a criminal but don’t know some clues about him, so they promise to prize the person who provides the most important clue after the criminal is arrested. A person may provide the police with something, but he is not certain that his message is the most important one during the process. So he can first sign the message anonymously and later he can prove to the police that it is he who provide the important clue after the message is announced to be the most important one.

The paper is organized as following: In section 2, we introduce some related knowledge that will be used in our scheme; In section 3, we present our verifiable ring signature; In section 4, we give a simple cryptanalysis of our scheme. The final section of the paper is a conclusion.

This paper is published in CANS’03 --- Third International Workshop on Cryptology and Network Security, DMS Proceedings, pp. 663-665, U.S.A, September 2003
2 Related Works

2.1 Witness Indistinguishable Signatures[7]

Let \( p_i, q_i \) be large primes, \( g_i \) be a base point of \( GF(p_i) \) whose order is \( q_i \).

Let \( x_i, y_i \) be \( y_i = g_i^{x_i} \mod p_i \). Here \( x_i \) is the private key and \( (y_i, p_i, q_i, g_i) \) is the public key. Let \( L \) be a set of \( (y_i, p_i, q_i, g_i) \) for \( i = 0, 1, \ldots, n - 1 \). Let \( h: \{0,1\}^* \rightarrow \{0,1\}^l \) be a publicly available hash function, where \( l \) is larger than the largest \( |q_i| \).

A signer who owns private key \( x_i \) generates a signature for message \( M \) with public key list \( L \) that includes his own public key, in the following way.

Simulation step: For \( i = 0, 1, \ldots, n - 1, i \neq s \), select \( c_i \) from \( GF(q_i) \) and compute \( z_i = g_i^{x_s} y_i^{c_i} \mod p_i \):

Real proof step: Select \( r_s \) from \( GF(q_s) \) and computes

\[
\begin{align*}
   z_s &= g_s^{r_s} \mod p_s \\
   c &= h(L, M, z_0, \ldots, z_{n-1}) \\
   c_s &= c \oplus (c_0 \oplus \cdots \oplus c_{s-1} \oplus c_{s+1} \oplus \cdots \oplus c_{n-1}) \quad (\oplus: \text{bitwise XOR}) \\
   s_s &= r_s - c_s \cdot x_s \mod q_s.
\end{align*}
\]

The resulting signature is \( \sigma = (c_0, s_0, \ldots, c_{n-1}, s_{n-1}) \).

A \((L, M, \sigma)\) is valid if

\[
   c_0 \oplus \cdots \oplus c_{n-1} = H(L, M, g_0^{x_0} y_0^{c_0} \mod p_0, \ldots, g_{n-1}^{x_{n-1}} y_{n-1}^{c_{n-1}} \mod p_{n-1}).
\]

2.2 RSA-Based Ring Signatures[1]

Let \( f_i : \{0,1\}^l \rightarrow \{0,1\}^l \) be a trapdoor one-way permutation where its inverse, \( f_i^{-1} \), can be computed only if the trapdoor information is known. Let \( E, D \) be a symmetric-key encryption and decryption function whose message space is \( \{0,1\}^l \).

Let \( h \) be a hash function whose output domain matches to the key-space of \( E, D \).
Given \( f_0, \ldots, f_{n-1} \), the signer who can compute \( f_s^{-1} \) generates a signature, for message \( M \) in the following way,

**Initialization:** Randomly selects \( c_0 \) from \( \{0,1\}^l \) and computes \( r_{n-1} = D_k(c_0) \) where \( k = h(M) \);

**Forward sequence:** For \( i = 0, \ldots, s-1 \), randomly selects \( s_i \) from \( \{0,1\}^l \) and computes \( c_{i+1} = E_k(c_i \oplus f_i(s_i)) \);

**Backword sequence:** For \( i = n-1, \ldots, s+1 \), randomly selects \( s_i \) from \( \{0,1\}^l \) and computes \( r_{i-1} = D_k(r_i \oplus f_i(s_i)) \);

**Shaping into a ring:** Computes \( s_i = f_s^{-1}(c_i \oplus r_i) \).

The resulting signature is \( (c_0, s_0, s_1, \ldots, s_{n-1}) \).

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 \( i = 0, \ldots, n-1 \).

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 is 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 \( \{0,1\}^b \). Each such combining function uses \( E_k \) as a sub-procedure, and produces as output a value \( z \) in \( \{0,1\}^b \), such that given any fixed values for \( k \) and \( v \). Each such combining function has the following four 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 \( C_{k,v}(y_1, y_2, \cdots, y_r) \) is a one-to-one mapping from \( y_s \) to the output \( z \).

2. Efficiently solvable for any single input: For each \( s, 1 \leq s \leq r \), 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 \( C_{k,v}(y_1, y_2, \cdots, y_r) = z \).
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

$$C_{k,v}(g_1(x_1), g_2(x_2), \cdots, g_r(x_r)) = z \quad \text{for} \quad x_1, x_2, \cdots, x_r$$

if the adversary can’t invert any of the trap-door functions $g_1, g_2, \cdots, g_r$.

3 Our Verifiable Ring Signature

Before proceeding, we assume the existence of a publicly defined symmetric encryption algorithm $E$ such that for any key $k$ of length $l$, the function $E_k$ is a permutation over $b$-bit strings. And we also assume the existence of a publicly defined collision-resistant hash function $h$ that maps arbitrary inputs to strings of length $l$, which are used as keys for $E$.

3.1 Key Generation

Each ring member, such as the $i$-th member $A_i$ of the ring members does the following,

Let $p_i$ be a prime such that it is hard to compute discrete logarithms in $GF(p_i)$,

$q_i$ be a prime divisor of $p_i - 1$, $o_i$ be a large prime divisor of $q_i - 1$, $g_i$ be a base point of $GF(p_i)$ whose order is $q_i$; The private key of $A_i$ is $x_{A_i}$ that meets $x_{A_i} < q_i$ and the corresponding public-key is $(y_{A_i}, p_i, q_i, g_i)$ where $y_{A_i} = g_i^{x_{A_i}} \mod p_i$.

3.2 DL-Based Trapdoor Functions

The trap-door function $g_i(\alpha, \beta)$ is defined as $g_i(\alpha, \beta) = \alpha \cdot y_{A_i}^\alpha \cdot g_i^\beta \mod p_i$,

its inverse function $g_i^{-1}(y)$ is defined as $g_i^{-1}(y) = (\alpha, \beta)$, where

$$\alpha \equiv y \cdot g_i^{-K} g_i^K \mod p_i, \quad \text{(1)}$$

$$\alpha^* = \alpha \mod q_i, \quad \text{(2)}$$

$$\beta \equiv x_{A_i} \alpha^* - K \cdot g_i^K \mod q_i, \quad \text{(3)}$$
3.3 Signature Generation

Step 1. First, the signer, $A_s$, computes the symmetric key $k$ as the hash of the message $M$ to be signed: $k = h(M)$

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

Step 3. Third, the signer, $A_s$, picks random $(\alpha_i, \beta_i)$ for all the other ring members $(1 \leq i \leq r, i \neq s)$ uniformly and independently, and computes $y_i = g_i(\alpha_i, \beta_i)$.

Step 4. Fourth, the signer, $A_s$, solves the following equation for $y_s$:

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

Step 5. Fifth, the signer, $A_s$, uses his knowledge of his trap-door function in order to invert $g_s^{-1}(y)$ on $y_s$ to obtain $(\alpha_s, \beta_s) = g_s^{-1}(y_s)$.

First, chooses a random integer $K(< q)$, computes $\alpha_s$ by equation 1, and keeps $K$ secret;

Second, computes $\alpha_s^*$ by equation 2;

Finally, computes $\beta_s$ by equation 3.

Step 6. The signature on the message $M$ is

$$\langle A_1, A_2, \cdots, A_r; v; (\alpha_1, \beta_1), (\alpha_2, \beta_2), \cdots, (\alpha_s, \beta_s) \rangle.$$

3.4 Signature Verification

Step 1. First, the verifier for $i = 1, 2, \cdots, r$, computes $y_i = g_i(\alpha_i, \beta_i)$.

Step 2. Second, the verifier hashes the message $M$ to compute the encryption key $k$:

$$k = h(M);$$

Step 3. Finally, the verifier checks that the $y_i$’s satisfy the fundamental equation:

$$C_{k,v}(y_1, y_2, \cdots, y_r) = v.$$
If the above equation holds, the verifier accepts the signature as valid. Reject otherwise.

### 3.5 Signer Verification

If the actual signer, $A_s$, is willing to prove to the verifier that he actually signs the signature, then he does the following,

**Step 1.** First, the signer $A_s$ sends secretly the secret integer $g_s^K$ to the verifier;

**Step 2.** Second, the verifier checks that if the $g_s^K$ satisfies the equation:

$$\alpha_s \equiv y \cdot (g_s^K)^{-s_s} \mod p_s.$$  

If $\alpha_s \equiv y \cdot (g_s^K)^{-s_s} \mod p_s$, the verifier accepts that $A_s$ is the real signer. Reject otherwise.

### 4 Cryptanalysis of the Scheme

First, the adversary can randomly choose an integer $s, 1 \leq s \leq r$, and a $b$-bit value $v$ and then he can chooses all the $(\alpha_i, \beta_i)$ except $(\alpha_s, \beta_s)$. By the definition of trap-door functions, he can computes all the $y_i$ except $y_s$ according to $(\alpha_i, \beta_i)$; Then he can compute $y_s$ from $C_{k,v}(y_1, y_2, \cdots, y_r) = v$; But because he doesn’t know the secret keys $x_{A_s}$, so he will face the DL problem when he solves $(\alpha_s, \beta_s)$ from $y_s$. However, he can guess a pair $(\alpha_s', \beta_s')$, but the probability of success is $\frac{q_s}{p_s \cdot q_s} = \frac{1}{p_s}$. Because $p_s$ is a large prime, the probability is negligible.

The adversary can always obtain $y_s$ and $(\alpha_s, \beta_s)$, but when he wants to solve the secret keys $x_{A_s}$ from $y_s$ and $(\alpha_s, \beta_s)$, he must again face the DL problem of solving $K \cdot g_s^K$ from $g_s^{-K} g_{s_s}^K$.

As for the security of Signer Verification, it is obviously a DL problem if a person wants to fake the actual signer. Though the verifier could get the $g_s^K$ in the process of signer verification, he couldn’t get the secret keys $x_{A_s}$, for he can’t get $K \cdot g_s^K$ from $g_s^K$. 
It should be stressed that the signer, $A_s$, should choose different random $K$
eq every time when he signs. Otherwise, if the verifier receives two same $g_s^K$ form two signatures signed by $A_s$, he can get the following two equations:

\[
K \cdot g_s^K = x_{A_s} \alpha + \beta \mod q_s
\]

\[
K \cdot g_s^K = x_{A_s} \alpha^* + \beta^* \mod q_s
\]

Then, the verifier can solve out $A_s$‘s private key $x_{A_s}$.

From above, our proposed ring signature satisfies:

- **Signer-ambiguity** that it is infeasible to identify who among the possible signers generates a signature;
- **Unforgeability** that the signature can only be produced by one of the ring members;
- **Verifiability** that the verifier can be convinced who is the real signer if the signer wants to reveal himself.

5 Conclusions

We propose a verifiable ring signature which has not only all the properties of a ring signature, but the property that the verifier can correctly determine who among the possible signers actually signs the signature if the signer is willing to reveal that it is he who signs the signature.

Acknowledgment: This work was supported by National 973 Project Foundation of China (G1999035804).

References