Applied Mathematical Sciences, Vol. 1, 2007, no. 32, 1551 - 1562

A Novel Identity-Based Society Oriented Signature Scheme with Anonymous Signers

Hui-Feng Huang*

Department of Information Management
National Taichung Institute of Technology, Taichung 404, Taiwan, R.O.C.
phoenix@ntit.edu.tw

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University, Taichung 40724, Taiwan, R.O.C.
ccc@cs.ccu.edu.tw

Abstract

Recently, Saeedina proposed an identity-based society oriented signature scheme with anonymous signers based on the Quillou-Quisquater signature scheme. The scheme is identity-based and the signatures are verified with respect to only one identity. The verifier does not have to know the identities of the co-signers, but just that of the organization they represent. The society signature is verified like an ordinary signature. Saeedina claimed that his scheme can overcome two difficulties which usually occur in society signature schemes. (1) Each user may participate in different organizations at the same time and can sign messages for different organizations with his unique secret key. (2) The public verification key of the organization can remain the same while some co-signers leave or join the organization. However, in 2003, Shao showed that Saeedina's society signature scheme is not secure. In this paper, we propose a new society signature scheme with anonymous signers based on RSA cryptosystem. Our scheme can easily overcome the above two difficulties. Furthermore, due to the simplicity feature and fewer parameter requirements, the proposed scheme is very suitable for today's applications.

---

* Corresponding author

Keywords: RSA cryptosystem, society signature

1. Introduction

The concept of society oriented cryptography was first introduced by Desmedt [1]. A society oriented signature is essentially like an ordinary single signature except that is created by several individuals, simultaneously. There are two kinds of society signature schemes: with known signers and with anonymous signers.

The first type of society signature schemes is commonly referred to as multisignature scheme. It allows multiple signers to sign the same document separately and then combines these individual signatures into a multisignature. The receiver who wishes to verify the document is actually signed by those known signers. The verification process of a multisignature should be almost identical to the verification process of an individual's signature. There have been many multisignature schemes proposed in some literatures [4, 5, 6].

For the second type of society signature schemes, the verifier only knows that the signature originated from some organization and verifies its correctness with respect to a single identity and a fixed master public key of the organization. That is, the society signature is verified exactly in the same way as an ordinary signature. For the verifier, it is not necessary to know the actual co-signers or even how many people have cooperatively signed the message. From the organization's point of view, however, it should be guaranteed that all those responsible for creating a signature on behalf of the organization are present and contribute actively. In other words, no valid signature can be produced if at least one of the co-signers is not participating. The society signature with anonymous signers is an important technique of modern cryptography. For example, let us consider the common circumstance of using a credit card. As a vendor, we only verify if this is a valid credit card from a card issuer. It's unnecessary to verify if the credit card has been authorized by the group of people who approve to issue this credit card.

Now, there are two difficulties with such society signature schemes with anonymous signers, they are as follows:

(1) When some members leave or join the organization to cooperatively sign messages, or more generally, when the internal composition of the organization changes, the public verification key of the organization should remain the same. Since the organization is known to the world by its identity, any modification in its membership should be transparent for outsiders.

(2) When an individual participates in several organizations at the same time, he can

sign messages for different organizations with the same secret key.

To overcome the two problems, Saeedina [8] recently proposed an identity-based society oriented signature scheme with anonymous signers based on the Quillou-Quisquater signature scheme [2, 3]. However, in 2003, Shao [9] shows that Saeedina's scheme suffers from some weakness. For instance, if some members of a given group leave or if some new members join, then the secret keys of the signers would be revealed.

In this paper, we propose a new identity-based society oriented signature scheme with anonymous signers based on RSA signature scheme [7].Owing to its simplicity and fewer parameter requirements, the RSA system still remains the most popular cryptosystem and is adopted as a standard worldwide. In the proposed method, each user may participate in different organizations at the same time and sign messages for different organizations with his unique secret key. In addition, if some members leave or join the organization, the remaining persons can still sign messages with their unique secret keys without even fearing any change in the structure of the organization. Also, the public verification key for the verifier is the same. In this way, it is very convenient for any verifier to verify the society signature with respect to the organization and each signer can dynamically join in different groups. Hence, the proposed scheme can easily overcome the above two problems. Therefore, the properties of simplicity, efficiency and flexibility make our scheme very attractive in many electronic applications.

The rest of this paper is organized as follows. In the next section, we briefly describe some related work. In Section 3, we introduce the proposed society oriented signature scheme with anonymous signers. The security analysis and the performance of the proposed scheme are discussed in Section 4. Finally, a brief conclusion is made in Section 5.

2. Related Works

Before we depict the new threshold proxy signature scheme, we state related works that will allow us to discuss its security in Section 4.

In the typical RSA digital signature scheme [7], the modulus $N'= p'\times q'$ is publicly known, where $p'$and $q'$are two secret large primes. For the security of RSA cryptosystem, it is difficult to factor N' into $p'$and q'. A signer randomly selects a private signing key $d'$and computes its corresponding public verification key e' so that $e'\times d' =1 \mod \phi(N')$, where $\phi(N') = (p'-1)(q'-1)$ is kept secretly.

Like all identity based schemes, our proposal has a trusted authority (TA) that is

responsible for generating the secret keys for the users in the system. Before generating the keys, TA randomly chooses two large prime numbers p_1 and p_2 such that these integers p_1 and p_2 are greater than 2^{256}. Here another two secret prime numbers n_1 and n_2 have to be computed, such that $n_1 = 2p_1 + 1$ and $n_2 = 2p_2 + 1$. An integer N is defined as the product of n_1 and n_2. That is $N = n_1 \times n_2$. Next, TA selects a secret key d and its corresponding public key e such that $e \times d = 1 \mod (p_1 \times p_2)$. Then, the parameters N, e, and a one-way hash function $h(\ )$ are published, and the parameters $d, \phi(N), n_1$, and n_2 are kept secretly. It is easy to see that $\phi(N) = (n_1 - 1)(n_2 - 1) = 4 \times (p_1 \times p_2)$. Since $e \times d = 1 \mod (p_1 \times p_2)$, there exists some integer k such that $e \times d = k \times (p_1 \times p_2) + 1$. Hence, we can obtain

$$4 \times e \times d = 4 \times k \times (p_1 \times p_2) + 4 = k\phi(N) + 4.$$

In this way, we have $(m^{4d})^e = m^4 \mod N$, for $m \in Z_N^*$.

Now, every user U_i in the system receives a secret key $s_i = (4d)^{I_i} \mod p_1 \times p_2$ which is computed by TA, where I_i is U_i's identity number. After receiving s_i, U_i can verify the validity of his secret key s_i by checking the following equality

$$(b^{s_i})^{e^{I_i}} = (b^{(4d)^{I_i}})^{e^{I_i}} = (b^{(4de)^{I_i}} = b^{4^{I_i}} \mod N,$$

where $b \in Z_N^*$ is randomly selected by U_i.

3. The Proposed Scheme

In this section, based on RSA cryptosystem, we describe a novel identity-based society oriented signature scheme with anonymous signers. The proposed scheme consists of three stages: (1) the organization's secret key generation stage, (2) the society signature generation stage, and (3) the verification stage. In the organization's secret key generation stage, TA (trusted authority) generates the organization's secret key. In the society signature generation stage, all the co-signers of the organization cooperatively create a valid society signature for a message. In the verification stage, the verifier can identify the society signature to sign on behalf of the organization with the organization's public key. The details of the new scheme are depicted as follows.

The organization's secret key generation stage:

Suppose that an organization G with identity number I_G wishes to enable a number of its k members $\{U_1, U_2, \cdots, U_k\}$ to co-sign documents on its behalf. Then,

TA computes the organization's secret key $s_G = (4d)^{I_G} \mod p_1 \times p_2$ and performs the following steps.

1. TA uses k distinct points $(1, s_1), (2, s_2) \ldots, (k, s_k)$ to generate the secret polynomial f of degree k of the form

$$f(x) = ((k+1)!)^{-1} \times r \times s_G + a_1 x + a_2 x^2 + \cdots + a_k x^k \mod (p_1 \times p_2),$$

where the random prime number r is randomly selected by TA.

It is obvious that coefficients $a_1, a_2, \cdots, a_k$ can be uniquely determined by using these k distinct points $(1, s_1), (2, s_2) \ldots, (k, s_k)$.

2. TA computes $c = (k+1)! f(k+1) \times \prod_{i=1, i \neq k+1}^{k+1} \frac{-i}{k+1-i} \mod (p_1 \times p_2)$ and gives back c and r to the organization G.
3. Finally, TA publishes the current values c and r.

The society signature generation stage:

Without loss of generality, the k co-signers of G want to cooperatively sign a message M on behalf of the organization G. Then, they perform the following tasks to generate the signature for the message M.

1. Using the concept of RSA signature scheme [7], each U_i constructs the partial signature z_i of M with his secret key s_i as follows.

$$z_i = h(M)^{L_i \times s_i} \mod N,$$

where $L_i = ((k+1)!) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}$ is an integer. Then, each U_i sends z_i to the combiner. The combiner can be the secretary of the organization G or someone randomly selected from the set $\{U_1, U_2, \cdots, U_k\}$.

2. The combiner of G confirms the validity of z_i by checking whether or not $(z_i)^{e^{I_i}} = h(M)^{L_i \times 4^{I_i}} \mod N$, where $L_i = ((k+1)!) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}$. If all z_i for $i = 1, 2, \ldots, k$ are verified, then the combiner computes $Z = w \times \prod_{i=1}^{k} z_i \mod N$, where $w = h(M)^c \mod N$.
3. Finally, Z is the society signature of the message M.

In fact, the society signature Z of the message M is computed as $Z = h(M)^{r \times s_G} \mod N$. In this stage, it is easy to see that these k co-signers sign the message without revealing their secret signing key s_i. Therefore, in our method, the signing key s_i

can be used repeatedly during its valid period.

The verification stage:

To verify the validity of the signature actually with respect to the organization *G*, the verifier examines the following steps with those parameters N, e, I_G, *r*, and a one-way hash function $h(\ )$.

1. Any verifier confirms the current value *r* which is made public by TA now.
2. To make sure the society signature *Z* of *M* is indeed signed by *G*, the verifier checks the following equation with the organization *G*'s public key I_G or e^{I_G}:

$$(Z)^{e^{I_G}} = h(M)^{r\times 4^{I_G}} \bmod N . \qquad (1)$$

If Equation (1) holds, the verifier is convinced that the valid signature *Z* of *M* is equivalent to the signature from the organization *G*. It is obvious that the society signature is verified the same as an ordinary signature. For the security of organization signature, the random prime number *r* should not be reused with different sets of co-signers.

The following theorem shows the signature *Z* of the message *M* is produced by the proposed scheme satisfies $(Z)^{e^{I_G}} = h(M)^{r\times 4^{I_G}} \bmod N$.

Theorem 1: If the signature *Z* of *M* is true with respect to the organization *G*, then $(Z)^{e^{I_G}} = h(M)^{r\times 4^{I_G}} \bmod N$ holds.

Proof: Let $\{U_1, U_2, \cdots, U_k\}$ be a set of *k* members in *G*, and their signing secret key $s_i = (4d)^{I_i} \bmod p_1 \times p_2$, where I_i is U_i's identity number. A polynomial *f* of degree *k* is constructed by *k* distinct points $(1, s_1), (2, s_2), \ldots, (k, s_k)$ as:

$$f(x) = ((k+1)!)^{-1} \times r \times s_G + a_1 x + a_2 x^2 + \cdots + a_k x^k \bmod (p_1 \times p_2), \qquad (2)$$

where $s_G = (4d)^{I_G} \bmod p_1 \times p_2$ is the secret key of the organization *G* and I_G stands for the identity number of *G*. It is obvious that coefficients $a_1, a_2, \cdots, a_k$ can be uniquely determined by using these *k* distinct points $(1, s_1), (2, s_2) \ldots, (k, s_k)$. We note that $f(i) = s_i$ for $i = 1,2,\ldots,k$. TA can compute $c = (k+1)!\, f(k+1) \times \prod_{i=1, i\neq k+1}^{k+1} \frac{-i}{(k+1-i)} \bmod (p_1 \times p_2)$ by Equation (2). According to Equation (2), we can obtain

$$r \times s_G = ((k+1)!) f(0). \quad (3)$$

Because a polynomial f can be derived by the following Lagrange formula:

$$f(x) = \sum_{i=1}^{k+1} [f(i) \times \prod_{j=1, j \neq i}^{k+1} \frac{x-j}{i-j}] \mod p_1 \times p_2. \quad (4)$$

From Equations (3) and (4), we have

$$r \times s_G = ((k+1)!) \times f(0) = ((k+1)!) \times \sum_{i=1}^{k+1} [f(i) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}] \mod p_1 \times p_2. \quad (5)$$

On the other hand, from the proposed method, $Z = w \times \prod_{i=1}^{k} z_i \mod N$, where $w = h(M)^c \mod N$, $z_i = h(M)^{L_i \times s_i} \mod N$, and $L_i = ((k+1)!) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}$.

Therefore, according to the proposed scheme and Equation (5), we have

$$\begin{aligned}
(Z)^{e^{I_G}} &= (w \times \prod_{i=1}^{k} z_i)^{e^{I_G}} && \mod N \\
&= \{h(M)^{((k+1)!) \times \{\sum_{i=1}^{k+1} [f(i) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}]\}}\}^{e^{I_G}} && \mod N \\
&= \{h(M)^{((k+1)!) \times f(0)}\}^{e^{I_G}} && \mod N \\
&= h(M)^{r \times s_G \times e^{I_G}} && \mod N \\
&= h(M)^{r \times (4d)^{I_G} \times e^{I_G}} && \mod N \\
&= h(M)^{r \times 4^{I_G}} \mod N, \text{ where } 4d \times e = 4 \mod \phi(N).
\end{aligned}$$

Hence, the theorem is proved.

In the proposed scheme, $p_1 \times p_2 = \frac{1}{4}\phi(N)$ is a secret parameter, and $\prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}$ is not sure to be an integer. Thus, in our method, U_i can construct his partial signature $z_i = (h(M))^{s_i \times L_i} = (h(M))^{f(i) \times ((k+1)!) \times \prod_{j \in B, j \neq i} \frac{-j}{i-j}} \mod N$,

where $f(i) = s_i$, and $L_i = ((k+1)!) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{j-i}$ is an integer.

From our proposal, each user may participate in different organizations (within the same organization or not) with his unique secret key. Moreover, if some signers of a given organization leave the organization or if some new signers join the organization, the remaining members can still sign documents with their unique secret key and the

organization's public key is also fixed for any verifier to verify the society signature, without even being aware of any change in the structure of the organization. The only modified values *c* and *r* are made public. The updating algorithm for both of the addition and deletion of signers in the organization is alike. Now, we only depict the addition of signers in the organization as follows.

Adding a co-signer: Suppose a new person U_{k+1} joins the existing set of co-signers set $\{U_1, U_2, \cdots, U_k\}$ of the organization *G*. In our organization's secret key generation stage, TA firstly discards the old values *c* and *r*, and then uses *k*+1 distinct points $(1, s_1), (2, s_2) \ldots, (k, s_k), (k+1, s_{k+1})$ to generate the secret polynomial f' of degree *k*+1 of the form

$$f'(x) = ((k+2)!)^{-1} \times r' \times s_G + b_1 x + b_2 x^2 + \cdots + b_{k+1} x^{k+1} \mod (p_1 \times p_2)$$,where

r' is a different random prime number chosen by TA.

Next, TA computes $c' = (k+2)! f(k+2) \times \prod_{i=1, i \neq k+2}^{k+2} \frac{-i}{k+2-i} \mod (p_1 \times p_2)$ and gives back c' and r' to the organization *G*. Finally, TA claims the current values c' and r'. The other information in the system stays the same. Thus, according to our society signature generation stage, these *k*+1 co-signers can cooperatively create the society signature, then, in the verification stage, any verifier can verify the validity of the signature with respect to the organization *G* by using the organization's public key e^{I_G} and the current value r'.

4. Discussions

In this section, we discuss the security and the performance of the proposed identity-based society oriented signature scheme with anonymous signers.

4.1 Secrecy

In the proposed scheme, both signing and verification are based on RSA cryptosystem. The security of RSA cryptosystem is founded in the difficulty of the integer factoring problem. For $e \times d = 1 \mod (p_1 \times p_2)$, where $p_1 \times p_2 = \frac{1}{4}\phi(N)$, then, from the system's public key *e*, one cannot derive the system private key *d*, since the parameter $(p_1 \times p_2)$ is unknown. On the other hand, although the organization *G*'s secret key $s_G = (4d)^{I_G} \mod (p_1 \times p_2)$ is created by TA, the organization cannot compute the system's private key *d*, since the parameters p_1 and p_2 are unknown. Even if all *k* co-signers of *G* conspire to obtain the group

secret key s_G, without knowing $(p_1 \times p_2)$ they also cannot derive the system's private key *d*. Therefore, the system's private key *d* can be kept secret and reused with different organizations. Without knowing the private key *d* of the system, it is difficult to obtain any signer's secret key s_a from the signer U_a's identity number I_a, where $s_a = (4d)^{I_a} \mod (p_1 \times p_2)$.

By applying Lagrange interpolating polynomial, the polynomial *f* of degree *k* requires at least *k*+1distinct points, namely $(x_i, f(x_i))$, to reconstruct the organization *G*'s signing key $r \times s_G = ((k+1)!) \times f(0)$, where there are *k* co-signers in *G*. In other words, *k* or fewer points cannot reconstruct *G*'s signing key. In our scheme, TA uses *k* distinct points $(1, s_1), (2, s_2) \ldots, (k, s_k)$ to create the secret polynomial *f* of degree *k* of the form

$$f(x) = ((k+1)!)^{-1} \times r \times s_G + a_1 x + a_2 x^2 + \cdots + a_k x^k \mod (p_1 \times p_2),$$ where s_j is the co-signer U_j's secret key for $j = 1,2,\cdots,k$. Then, TA can compute $c = (k+1)! f(k+1) \times \prod_{i=1, i \neq k+1}^{k+1} \frac{-i}{k+1-i} \mod (p_1 \times p_2)$ and then publishes the current value *c*. It is obvious that

$$f(k+1) = c \times \{(k+1)! \prod_{i=1, i \neq k+1}^{k+1} \frac{-i}{k+1-i}\}^{-1} \mod (p_1 \times p_2). \quad (6)$$

However, it is very hard for any one to derive *f*(*k*+1) from Equation (6) because that $(p_1 \times p_2)$ is unknown. In this situation, even if all *k* co-signers of *G* reveal their secret key s_j's, without knowing *f*(*k*+1), they also cannot derive the secret signing key $r \times s_G = ((k+1)!) \times f(0)$. Without $r \times s_G$, no one can forge the society signature on behalf of the organization *G*. For the security of the proposed method, we consider some possible attacks.

1. Without the U_i's signing key s_i, based on RSA signature scheme, no one can forge the signer U_i to generate the signature $z_i = h(M)^{L_i \times s_i} \mod N$ of the message *M*, where $L_i = ((k+1)!) \times \prod_{j=1, j \neq i}^{k+1} \frac{-j}{i-j}$ is an integer. Suppose that an attacker knows one signature z_i for a message *M*, where $z_i = h(M)^{L_i \times s_i} \mod N$. However, based on the

discrete logarithms, the attacker cannot derive s_i from z_i.

2. Without the organization *G*'s secret key s_G , no one can create a valid signature on behalf of the organization *G*. Based on the Lagrange interpolation formula, we cannot construct $r \times s_G = ((k+1)!) \times f(0)$ from the polynomial *f* of degree *k* if only fewer than *k*+1 points show up. On the other hand, suppose that an attacker knows one signature *Z* for a message *M*, where $Z = h(M)^{r \times s_G} \bmod N$. Based on the discrete logarithms, the attacker cannot derive $r \times s_G$ from *Z*.

3. Given a pair of valid society signatures Z and Z' for messages M_1 and M_2 produced by the proposed protocol, respectively, we have

$$\begin{aligned} & (Z)^{e^{I_G}} \times (Z')^{e^{I_G}} && \bmod N \\ &= (Z \cdot Z')^{e^{I_G}} && \bmod N \\ &= h(M_1)^{r \times 4^{I_G}} \times h(M_2)^{r \times 4^{I_G}} && \bmod N \\ &= [h(M_1) \times h(M_2)]^{r \times 4^{I_G}} && \bmod N . \end{aligned}$$

If the intruder computes $Z'' = Z \times Z' \bmod N$ and tries to derive the valid society signature for some message, then according to the proposed scheme, he has to find M_3 such that $h(M_3) = h(M_1) \times h(M_2) \bmod N$. That is, $(Z'')^{e^{I_G}} = h(M_3)^{r \times 4^{I_G}} \bmod N$. However, M_3 is protected under the one-way hash function $h(\ )$, so the probability of obtaining M_3 such that $h(M_3) = h(M_1) \times h(M_2) \bmod N$ is equivalent to performing an exhaustive search on M_3. Therefore, the proposed scheme ensures that a valid society signature would be generated only when *k* signers can cooperatively sign the message on behalf of the organization *G*. Moreover, the organization verification key e^{I_G} is computed from the organization *G's* identity number I_G, where *e* is a public parameter of the system. Hence, the group *G* cannot deny having generated the valid society signature.

4. If all co-signers $\{U_1, U_2, \cdots, U_k\}$ of *G* leave the organization, they can still continue to cooperatively sign the signature Z' of the message M' such that $Z' = h(M')^{r \times s_G} \bmod N$, where *r* is selected for these *k* co-signers. However, according to our proposal, the random prime number *r* should not be reused with different co-signers. Thus, *r* has been discarded by TA, now TA chooses and publishes another prime r' for new co-signers $U_1', U_2', \cdots, U_t'$ of *G* to create society

signature Z' of the message M' such that $Z' = h(M')^{r' \times s_G} \bmod N$. In this way, the co-signers $U_1, U_2, \ldots, U_k$ cannot obtain $(Z')^{\frac{r'}{r}} = (h(M')^{r \times s_G})^{\frac{r'}{r}} = h(M')^{r' \times s_G} \bmod N$ because r and r' are primes and $\phi(N)$ is unknown. Therefore, even if all co-signers $U_1, U_2, \ldots, U_k$ of G leave the organization they cannot cooperatively forge a signature on behalf of the organization.

4.2 Performance

With regard to efficiency, by using our proposal, one requires only the public keys such as the forms $e^{I_G}\ 4^{I_G}, e^{I_i}$, and 4^{I_i} to verify the validity of signature. Since e, 4, I_G and I_i are fixed in our scheme, one can pre-compute and store these values $e^{I_G}, 4^{I_G}, e^{I_i}$, and 4^{I_i} for speeding up the verification. For convenience, the following notations are used to analyze the computational complexity. T_e means the time for one exponentiation computation ; T_m defines the time for one modular multiplication computation ; T_h denotes the time for executing the adopted one-way hash function in one's scheme. Note that the times for computing modular addition and subtraction are ignored, since it is much smaller than T_e, T_m, and T_h.

In our scheme, suppose that there are k co-signers cooperatively to sign the society signature on behalf of the organization, then the computational complexity for each co-signer to generate his partial signature, the combiner to compute the society signature, and anyone to verify the society signature, are $T_e + T_m + T_h$, $(2k+1)T_e + (2k)T_m + T_h$, and $2T_e + T_m + T_h$, respectively. It is more efficient than Saeednia's scheme [8]. In addition to Saeednia's society signature scheme not being secure [9].

5. Conclusions

In this paper, we propose a novel society signature scheme with anonymous signers based on RSA cryptosystem. The society signature is verified the same as a single signature. Moreover, the proposed scheme can provide the following two properties:

(1) When some co-signers leave or add the organization, the public verification key of the organization stays the same. It does not affect the organization's public key.

(2) Each user may participate in different organizations to sign messages for different organizations with the same secret key based on his identity. It is very convenient to sign the message for the user.

Therefore, our identity-based society oriented signature scheme with anonymous signers is very suitable for many electronic transactions.

References

[1] Y. Desmedt, "Society and group oriented cryptography," *Advances in Cryptology, Proceedings of Crypto'87, Lecture Notes in Computer Science*, Springer-Verlag, 293(1988), 120-127.

[2] L. Guillou and J. J. Quisquater, "A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory," *Advances in Cryptology, Proceedings of EuroCrypto'88, Lecture Notes in Computer Science*, Springer-Verlag, 339(1989), 123-128.

[3] L. Guillou and J. J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge," *Advances in Cryptology, Proceedings of Crypto'88, Lecture Notes in Computer Science*, Springer-Verlag, 403(1989), 216-231.

[4] L. Harn, "Group-oriented (*t*,*n*) threshold digital signature and digital multisignature," *IEE Proceedings Computation Digital Technique*, 14(1994), 307-313.

[5] K. Ohta and T. Okamoto, "A digital multisignature scheme based on the Fiat-Shamir scheme," *Advances in Cryptology, Proceedings of Asiacrypt'91, Lecture Notes in Computer Science*, Springer-Verlag, 739(1993), 139-148.

[6] S. J. Park, S. W. Park, K. J. Kim, and D. H. Won, "Two efficient RSA multisignature schemes," International Conference on Information and Communications Security, *Proceedings of ICICS'97, Lecture Notes in Computer Science*, Springer-Verlag, 1334(1997), 217-222.

[7] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, 21(1978), 120-126, Feb.

[8] S. Saeednia, "An identity-based society oriented signature scheme with anonymous signers," *Information Processing Letters*, 83(2002), 295-299.

[9] Z. Shao, "Cryptanalysis of an identity-based society oriented signature scheme with anonymous signers," *Information Processing Letters*, 86(2003), 295-298.

Received: December 16, 2006