Improvement on Nominative Proxy Signature Schemes

Zuo-Wen Tan[1,2]
(Corresponding author: Zuo-Wen Tan)

Institute of Information & Management, Jiangxi University of Finance & Economics[1]
Nanchang 330013, Jiangxi Province, China (Email: tanzyw@163.com)
KLMM, AMSS of CAS, Beijing 100080, China[2]

(Received June 26, 2006; revised and accepted Oct. 3, 2006 & Nov. 8, 2006)

Abstract

In a nominative proxy signature scheme, an original singer delegates his signing power to a proxy signer, who generates a nominative signature on behalf of the original signer. In a nominative proxy signature scheme, only the nominee can verify the signature and if necessary, only the nominee can prove its validity to the third party. In this paper, we first classify the nominative proxy signature into two types, original-nominative proxy signature and proxy-nominative proxy signature. Then we analyze the nominative proxy scheme proposed by Park and Lee. We show that the scheme suffers from universal verification. We also point out that the scheme presented by Seo and Lee is insecure and the scheme cannot provide non-repudiation. Finally we present our nominative proxy signature schemes which overcome the weakness mentioned above.

Keywords: E-commerce, mobile communication, nominative signature, non-repudiation, proxy signature

1 Introduction

Digital signature is one of the most important techniques in modern information security system for its functionality of providing data integrity and authentication. A normal signature holds self-authentication property, that is, the signature can be verified by anyone who gains access to the signature. So the normal signature is not suitable for the situation where the message signed is sensitive to the signature receiver. To solve the problem, Kim, Park and Won introduced a new type of signature, nominative signature [5, 6]. Unlike a normal signature, only the nominee can verify directly the nominator(signer)'s signature and if necessary, only the nominee can prove to the third party that the signature is issued to him/her and is valid. Nominative signature is valuable in many application situations. Take electronic commerce for instance. A company sells its digital products over Internet. When a customer purchases a digital product, the customer would like to have the company's guarantee of quality, which is usually the merchant's signature. On the other hand, the company must prevent the customer from distributing the digital product to others.

In 1996, Mambo, Usuda and Okamoto [11] first introduced the concept of proxy signature. In a proxy signature scheme, an original signer delegates a user called proxy signer to sign message on behalf of the original signer. Since its introduction proxy signature has abstracted a great deal of interest. Now proxy signatures have found numerous applications, particularly in distributed computing, which include mobile agent application, mobile communication, and electronic voting, etc. Various proxy signature schemes have been presented [7, 8, 9], such as threshold proxy signatures [17, 19, 23], one-time proxy signatures [4, 22], multi-proxy signature [2], proxy multi-signature [3], proxy blind signature [10, 20], and proxy anonymous proxy signatures [16]. Mambo, Usuda and Okamoto [11] mentioned three types of delegation, full delegation, partial delegation and delegation by warrant. In the full delegation, the original signer gives its private key as the proxy signature key to the proxy signer. In the partial delegation, the original signer generates a delegation key by using a trap-door one-way function and its private key. Unlike the full delegation, the proxy signature is distinguishable from the original signer's normal signature. Partial delegation schemes can be further classified into proxy-unprotected partial delegation and proxy-protected partial delegation scheme. In proxy-unprotected partial delegation, the proxy signer uses the delegation key to sign on message. In proxy-protected partial delegation, the proxy signer generates the proxy signature using the delegation key and its private key. In delegation by warrant, the original restricts the proxy's signing ability by warrant which records the identities of the original signer and the proxy, the type of message delegated and the delegation period, etc. In the sequel, a proxy signature refers to a proxy-protected partial delegation signature.

In 2001, Park and Lee firstly introduce the concept nominative proxy signature and proposed a digital nominative proxy signature scheme [13]. Nominative proxy signature is a useful tool in the mobile communication environment. In the nominative proxy signature scheme for mobile communication, the mobile user acts as the original and the agent entity acts as the proxy signer. The nominative proxy signature is ascertained only by the nominee. Thus, the mobile user's and the agent entity's anonymity can be guaranteed. On the mobile communication, a mobile device always has less computational capability. The agent entity (proxy signer) with more computational power can perform some operations such as modular exponentiation on behalf of the mobile user to reduce the charge of mobile device. Recently, Dai et al. proposed a designated-receiver proxy signature for electronic commerce [1]. According to which of the original and the proxy the nominator is, we classifies nominative proxy signature into two types: original-nominative proxy signature and proxy-nominative proxy signature.

In this paper, we first analyze Park-Lee's nominative proxy scheme [13] and Seo-Lee's nominative proxy scheme [15]. As Seo and Lee claim, Park-Lee's scheme does not provide non-repudiation. The original signer or proxy signer can falsely deny later the fact he/she generates the signature. We showed that Park-Lee's nominative proxy signature is universally verifiable. That is, the nominative proxy signature is verified by anyone. We also showed Seo-Lee's scheme is insecure against the original signer's forgery. We finally present our nominative proxy signature schemes. Compared with G.-L. Wang's designated-verifier proxy signature scheme [21], the proposed schemes needs less communications and less computational cost.

The rest of this paper is organized as follows. In Section 2, we briefly review some properties of nominative proxy signature, then describe Park-Lee's scheme and gives its cryptanalysis. In Section 3, we recall Seo-Lee's nominative proxy signature scheme and analyze its security. In Section 4, we present our nominative proxy schemes and analyze its security and efficiency. Section 5 is dedicated to our conclusion.

2 Review on Park-Lee's Nominative Proxy Signature

2.1 Concept of Nominative Proxy Signature

In a nominative proxy signature, not the original signer but the proxy signer generates the nominative proxy signature and sends it to the signature receiver. A nominative proxy signature is called original-nominative proxy signature if the original is the nominator. A nominative proxy signature is called proxy-nominative proxy signature if the verifier is nominated by the proxy. They can be applied in different situations. For instance, the original-nominative proxy signature is suitable for mobile communications in which the receiver is chosen by the mobile user (the original signer), not by the agent entity (the proxy signer). While the proxy-nominative proxy signature is favorable to electronic commerce. On the e-commerce, the manufacturer acts as the original signer in order to provide the customer with quality guarantee. But the manufacturer need not take part in every vendition after the manufacture delegates the vendor. The vendor sells goods to the customers, so the signature receivers (the customers) is determined by the vendor. The nominator should be personated by the vendor (proxy entity).

A original-nominative proxy signature scheme satisfies the following requirements:

1) Only the original signer can nominate the receiver (verifier).

2) The original signer and the proxy signer cannot repudiate the nominative proxy signature after the signature is generated.

3) Only the nominee can directly verify the nominative proxy signature.

4) If necessary, only the nominee can prove to the third party that the nominative proxy signature is valid.

A proxy-nominative proxy signature should satisfy the Requirements 2), 3), 4) and the following condition:
$1'$) Only the proxy can nominate the receiver (verifier).

2.2 Description of Park-Lee's Nominative Proxy Signature

We will recall Park-Lee's nominative proxy signature [13]. The scheme involves three parties: the original signer **A**, the proxy signer **B** and the receiver **C**. Every entity has a public/private key pair $(x, y = g^x \mod p)$, where $x \in Z_q^*$, p is a large prime and q is a prime factor of $p-1$. The system parameters still include a public one-way hash function $H(\cdot)$. T is a time stamp and M is message. Through the paper, the system parameters is the same.

The nominative proxy signature scheme consists of the following phases.

1) **Proxy Generation:** **A** chooses a random $k \in_R Z_q$ and computes

$$\begin{aligned} r &= g^k (\mathrm{mod} p) \\ s_A &= x_A H(M||T) + kr (\mathrm{mod} q). \end{aligned}$$

2) **Proxy Delivery:** **A** sends (M, T, r, s_A) to the proxy signer **B** in a secure manner.

3) **Proxy Verification:** **B** computes $d = H(M||T)$ and checks if $g^{s_A} \overset{?}{=} y_A^d r^r (\mathrm{mod} p)$. If the equation holds, B accepts the delegation.

4) **Nominative Proxy Signature Generation:** **B** chooses $k_1, k_2 \in_R Z_q^*$ at random and computes

$$\begin{aligned} R &= g^{k_1 - k_2 x_B}(\bmod p), \\ Z &= y_C^{k_1}(\bmod p), \\ e &= H(y_C||R||Z||M), \\ s &= k_2 x_B - k_1 e s_A(\bmod q). \end{aligned}$$

The nominative proxy signature on message M is (M, T, r, R, Z, k_1, s).

5) **Nominative Proxy Signature Delivery:** **B** sends the signature (M, T, r, R, Z, k_1, s) to the verifier **C**.

6) **Verification of Nominative Proxy Signature:** **C** computes

$$\begin{aligned} d &= H(M||T), \\ e &= H(y_C||R||Z||M), \\ y_p &= y_A^d \cdot r^r(\bmod p). \end{aligned}$$

And then **C** verifies the nominative proxy signature by checking

$$(g^s \cdot y_p^{k_1 e} \cdot R)^{x_C} \overset{?}{=} Z(\bmod p).$$

2.3 Cryptanalysis of Park-Lee's Scheme

Park-Lee's scheme is a proxy-unprotected partial proxy signature scheme. The proxy signer's public key y_B is not be used during the signature verification, the scheme can not provide non-repudiation. In existence, the scheme is insecure against the original signer's forgery. The attack is as follows. A malicious original signer chooses $a, b, c, k_1 \in_R Z_q^*$ and computes

$$\begin{aligned} r &= g^a(\bmod p) \\ R &= g^b(\bmod p) \\ Z &= y_C^c \bmod p \\ d &= H(M||T) \\ e &= H(y_C||R||Z||M) \\ s &= c - x_A d k_1 e - b(\bmod q). \end{aligned}$$

Then, (M, T, r, R, Z, k_1, s) is a valid nominative proxy signature. This is because:

$$\begin{aligned} (g^s \cdot y_p^{k_1 e} \cdot R)^{x_C} &= [g^s \cdot (y_A^d r^r)^{k_1 e} \cdot g^b]^{x_C} \bmod p \\ &= [g^s \cdot g^{x_A d k_1 e} \cdot g^{a r k_1 e} \cdot g^b]^{x_C}(\bmod p) \\ &= g^{c x_C} = Z(\bmod p). \end{aligned}$$

Another original signer's forgery attack against Park-Lee's scheme can be found in [18].

Obviously, in Park-Lee's nominative proxy scheme, a secure channel must be kept between the original signer and the proxy signer. Otherwise, an adversary who have intercepted the delegation (M, T, r, s_A) can generate a nominative proxy signature as the malicious original signer **A** does.

Furthermore, Park-Lee's scheme does not satisfy the following requirement: only the nominee can verify the signature. Since the nominative proxy signature contains k_1, once anyone obtains the nominative signature (T, r, R, Z, k_1, s) on message M, he can validate the signature by checking the following:

$$g^s \cdot y_p^{k_1 e} \cdot R \overset{?}{=} g^{k_1}(\bmod p), y_C^{k_1} \overset{?}{=} Z(\bmod p).$$

3 Review on Seo-Lee's Nominative Proxy Signature

3.1 Description of Seo-Lee's Nominative Proxy Signature Scheme

The system parameters are the same as those in Park-Lee's scheme. Seo-Lee's scheme [15] is constructed as follows.

1) **Proxy Signature Key Generation Phase:** The phase is executed between the original signer **A** and the proxy **B**.

   a. **Proxy Generation:** **A** chooses a random $k \in_R Z_q \backslash \{0\}$, and computes $r = g^k(\bmod p)$, and $s_A = x_A \cdot H(M_w||r||T) + k \cdot r(\bmod q)$, where M_w is a warrant.

   b. **Proxy Delivery:** **A** sends (s_A, M_w, T, r) to the proxy signer **B**.

   c. **Verification and Alteration of the Proxy:** The proxy signer **B** validates the delegation by checking if the following holds

   $$g^{s_A} = y_A^{H(M_w||r||T)} \cdot r^r(\bmod p).$$

   If the above equation holds, **B** generates a proxy signature key s_p.

   $$s_p = s_A + x_B \cdot r(\bmod q).$$

2) **Nominative Proxy Signature Generation Phase:** This phase is executed between the proxy signer **B** and the nominee **C**.

   The proxy signer **B** chooses random integers $k_1, k_2 \in_R Z_q^*$, and computes:

   $$\begin{aligned} R &= g^{k_1 - k_2}(\bmod p) \\ Z &= y_C^{k_1}(\bmod p) \\ e &= H(M||M_w||y_C||R||Z) \\ s &= k_2 - e \cdot s_p(\bmod q). \end{aligned}$$

   Thus, **B** creates a nominative proxy signature $(M, M_w, T, y_C, r, R, Z, s)$. **B** transmits the nominative proxy signature to **C**.

3) **Nominative Proxy Signature Verification Phase:** The nominee **C** computes the proxy signature public key y_p.

$$\begin{aligned} e &= H(M||M_w||y_C||R||Z) \\ y_p &= y_A^{H(M_w||r||T)} \cdot (y_B \cdot r)^r (\mathrm{mod} p). \end{aligned}$$

And then, the nominee **C** verifies the nominative proxy signature by checking a congruence

$$(g^s \cdot y_p^e \cdot R)^{x_C} \overset{?}{=} Z(\mathrm{mod} p). \tag{1}$$

This is a proxy-nominative proxy signature. The scheme does not need a secure channel between the original signer **A** and the proxy signer **B**.

3.2 Cryptanalysis of Seo-Lee's Scheme

In this subsection, we analyze Seo-Lee's scheme. The scheme tries to overcome the weakness of Park-Lee's scheme. However, there exists a same weakness as Park-Lee's scheme holds. The scheme does not still provide non-repudiation. A dishonest original signer **A** can create a nominative proxy signature on behalf of the proxy signer **B**. We show the attack of the original signer's forgery in detail.

Proxy Signature Key Generation:
A chooses two random $a, b \in_R Z_q$ and computes the proxy signature key:

$$\begin{aligned} r &= y_B^{-1} g^a y_A^b (\mathrm{mod} p) \\ s_p &= x_A \cdot H(M_w||r||T) + a \cdot r + x_A \cdot b \cdot r (\mathrm{mod} q). \end{aligned}$$

Nominative Proxy Signature Generation:
The original signer **A** uses the proxy signature key s_p to produce the nominative proxy signature as the proxy signer B does in Seo-Lee's scheme.

Nominative Proxy Signature Verification:
After the nominee **C** receives the signature $(M, M_w, T, y_C, r, R, Z, s)$, **C** computes e, y_p and checks the Congruence (1). As a result, Congruence (1) holds. In other words, **A** forges a nominative proxy signature successfully. This is because:

$$\begin{aligned} g^{s_p} &= g^{x_A \cdot H(M_w||r||T) + ar + x_A br} \bmod p \\ &= y_A^{H(M_w||r||T)} \cdot g^{ar + x_A br} \bmod p \\ &= y_A^{H(M_w||r||T)} \cdot g^{ar} \cdot (r \cdot y_B \cdot g^{-a})^r \bmod p \\ &= y_A^{H(M_w||r||T)} \cdot (r \cdot y_B)^r \bmod p \\ &= y_p \bmod p. \end{aligned}$$

$$\begin{aligned} (g^s \cdot y_p^e \cdot R)^{x_C} &= (g^{k_2 - s_p e} \cdot y_p^e \cdot g^{k_1 - k_2})^{x_C} \bmod p \\ &= g^{k_1 x_C} \bmod p \\ &= Z \bmod p. \end{aligned}$$

In addition, a malicious original signer can frame the proxy signer by forging a nominative proxy signature on any message M. First, the original signer **A** randomly chooses a, b, d in Z_q^*. Then **A** computes

$$\begin{aligned} r &= y_B^{-1} g^a \bmod p \\ R &= g^b \bmod p \\ Z &= y_C^d \bmod p. \\ e &= H(M||M_w||y_C||R||Z) \\ s &= d - e(x_A H(M_w||r||T) + ar) - b \bmod q. \end{aligned}$$

Thus, $(M_w, T, y_C, r, R, Z, S)$ is a valid nominative proxy signature on message M. This is because:

$$\begin{aligned} e &= H(M||M_w||y_C||R||Z) \\ y_p &= y_A^{H(M_w||r||T)} \cdot (y_B \cdot r)^r (\mathrm{mod} p) \\ &= g^{x_A H(M_w||r||T) + ar} (\mathrm{mod} p). \end{aligned}$$

So, the following equations holds:

$$\begin{aligned} (g^s \cdot y_p^e \cdot R)^{x_C} &= (g^{s + e(x_A H(M_w||r||T) + ar) + b})^{x_C} \bmod p \\ &= y_C^{s + e(x_A H(M_w||r||T) + ar) + b} \bmod p \\ &= y_C^d \bmod p \\ &= Z. \end{aligned}$$

4 Proposed Nominative Proxy Signature Schemes

4.1 Two Nominative Proxy Signature Schemes

We first present our original-nominative proxy signature scheme. The system parameters are the same as those in Seo-Lee's scheme. The original-nominative proxy signature scheme comprises of the following phases.

.

Delegation Phase:

1) **Proxy Generation:** The original signer **A** generates a warrant m_w, which records the delegation limits of authority, valid period of delegation, and the identities of the original signer and proxy signer. **A** chooses a random $k \in_R Z_q^*$ and computes

$$\begin{aligned} r &= g^k (\mathrm{mod} p) \\ s_A &= x_A \cdot H(M_w||T||r||y_C) + k (\mathrm{mod} q). \end{aligned}$$

The original signer sends (m_w, T, r, y_C, s_A) to the proxy signer **B**.

2) **Delegation Verification:** After the proxy signer **B** receives the delegation warrant and delegation key (m_w, T, r, y_C, s_A), **B** checks wether $g^{s_A} = r y_A^{H(M_w||T||r||y_C)} (\mathrm{mod} p)$. If so, **B** begins to execute the proxy signature key generation algorithm. Otherwise, **B** refuses this delegation.

3) **Proxy Signature Key Generation:** The proxy signer **B** computes the proxy signature key:

$$s_p = s_A + x_B H(M_w||T||r||y_C)(\mathrm{mod} p).$$

Proxy Signature Generation Phase:
To generate an original-nominative proxy signature on message M, the proxy signer **B** does the same as in Seo-Lee's Scheme and generates a nominative proxy signature $(M, M_w, T, y_C, r, R, Z, s)$. Then the proxy signer **B** sends the signature to the nominee **C**.

Nominative Proxy Signature Verification Phase:
The verifier **C** first checks if message M signed conforms to the warrant M_w, then computes the proxy signature public key y_p.

$$y_p = g^{s_p} = r(y_A y_B)^{H(M_w||T||r||y_C)}(\text{mod} p).$$

And then, the nominee **C** verifies the nominative proxy signature by checking

$$(g^s \cdot y_p^e \cdot R)^{x_C} \overset{?}{=} Z(\text{mod} p), \qquad (2)$$

where $e = H(M||M_w||T||r||y_C||R||Z)$.

Nominative Proxy Signature Confirmation Phase:
If necessary, the nominee **C** (prover) proves the validity of the signature to the third party (verifier) **V**. The nominee **C** proves that $(g^s \cdot y_p^e \cdot R)^{x_C} = Z(\text{mod} p)$ and $g^{x_C} = y_C(\text{mod} p)$ in a zero-knowledge manner. The zero knowledge confirmation protocol is executed between **C** and **V** as follows.

1) **C** computes $u = g^s \cdot y_p^e \cdot R(\text{mod} p)$, and sends $(u, M, M_w, T, r, y_C, R, Z)$ to the verifier **V**.

2) **V** computes $e = H(M||M_w||T||r||y_C||R||Z)$ and checks if $u = g^s \cdot y_p^e \cdot R(\text{mod} p)$.

3) **C** proves to the verifier **V** that $log_u Z = log_g y_C$ in a zero knowledge fashion.

We can construct a proxy-nominative proxy signature scheme in a similar way. For completeness, we list the components of a proxy-nominative proxy signature scheme.

1) **Delegation Phase:** **A** computes: $k \in_R Z_q^*$,

$$\begin{aligned} r &= g^k(\text{mod} p) \\ s_A &= x_A \cdot H(M_w||T||r) + k(\text{mod} q). \end{aligned}$$

A sends (M_w, T, r, s_A) to **B**. Next, **B** checks $g^{s_A} \overset{?}{=} r \cdot y_A^{H(M_w||T||r)}(\text{mod} p)$ and then computes $s_p = s_A + x_B \cdot H(M_w||T||r)(\text{mod} q)$.

2) **Signing Phase:** B computes: $k_1, k_2 \in_R Z_q^*$,

$$\begin{aligned} R &= g^{k_1 - k_2}(\text{mod} p), \\ Z &= y_C^{k_1}(\text{mod} q) \\ e &= H(M||M_w||T||r||y_C||R||Z) \\ s &= k_2 - e \cdot s_p(\text{mod} q). \end{aligned}$$

Then **B** sends $(M, M_w, T, y_C, r, R, Z, s)$ to **C**.

3) **Verification Phase:** C checks:

$$\begin{aligned} y_p &= r \cdot (y_A y_B)^{H(M_w||T||r)}(\text{mod} p), \\ e &= H(M||M_w||T||r||y_C||R||Z) \\ (g^s \cdot y_p^e \cdot R)^{x_C} &\overset{?}{=} Z(\text{mod} p). \end{aligned}$$

4.2 Security Analysis of Proposed Schemes

We can make analysis of both the proposed nominative proxy signature schemes in a similar way. For simplification, we only present the analysis of the proposed original-nominative proxy signature scheme.

Firstly, the signature scheme does not require a secure channel between the original signer and the proxy signer.

Secondly, the nominative proxy signature scheme holds nonrepudiation. An original signer cannot forge any valid proxy signature key as mentioned in Section 3.2. It is intractable for the original signer to choose a proper r and compute s_p from the following the equation:

$$g^{s_p} = r(y_A y_B)^{H(M_w||T||r||y_C)}(\text{mod} p).$$

The proxy signature key s_p is in essence a Schnorr signature on message M_w using private key $(x_A + x_B)$. Schnorr signature scheme is provably secure [14]. Nor can the proxy signer produce a valid proxy signature key without participation of the original signer.

Next, in the proposed scheme, the nominee only can be nominated by the original signer. If the proxy signer nominates a nominee, the verification Equation (2) will not hold.

Recently Wang proposed a designated-verifier proxy signature scheme [21] based on Nicolosi et al.'s two-party Schnorr signature scheme [12]. In Wang's scheme, the proxy signer generates the proxy signature key s_p by running an interactive protocol with the original signer through three rounds of communication. In our scheme, the proxy signature key is generated through only one round of communication between the original signer and the proxy signer. Our scheme has less two modulo exponentiations than Wang's scheme.

5 Conclusion

In this paper, we classify the nominative proxy signature into original-nominative proxy signature and proxy-nominative proxy signature. Then we analyze Park and Lee's nominative proxy scheme. The scheme does not satisfy the foundational property of nominative proxy signature: only the nominee can verify the signature. It suffers from universal verification. We show that Seo and Lee's scheme is insecure against the original signer's forgery. Finally we present our nominative proxy signature schemes which hold all the properties of a nominative proxy signature scheme. Compared with the scheme recently proposed by Wang, our scheme is more efficient.

Acknowledgements

Supported by National Natural Science Foundation of China under Grant No. 10371127 and Science Research Fund of Hu Nan Province Education Department (05c261 and 05c262).

References

[1] J. Z. Dai, X. H. Yang, and J. X. Dong, "Designated-receiver proxy signature scheme for electronic commerce," in *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 384-389, IEEE, Oct. 5-8, 2003.

[2] S. J. Hwang, and C. H. Shi, "A simple multi-proxy signature scheme," in *Proceedings of the Tenth National Conference on Information Security*, pp. 134-138, 2000.

[3] S. J. Hwang, and C. C. Chen, "A new proxy multi-signature scheme," in *International Workshop on Cryptology and Network Security*, Sep. 2001.

[4] H. Kim, J. Baek, B. Lee, and K. Kim, "Secrets for mobile agent using one-time proxy signature," *Cryptography and Information Security*, vol. 2, no. 2, pp. 845-850, 2001.

[5] S. J. Kim, S. J. Park, D. H. Won, "Nominative signatures," in *Proceedings of the ICEIC'95*, pp. 68-71, 1995.

[6] S. J. Kim, S. J. Park, D. H. Won, "Zero-knowledge nominative signature," in *Proceedings of the International Conference on the Theory and Applications of Cryptology (Pragocrypt'96)*, pp. 380-392, 1996.

[7] S. J. Kim, S. J. Park, D. H. Won, "Proxy Signatures, revisited," *ICICS'97*, LNCS 1334, pp. 223-232, Springer-Verlag, 1997.

[8] B. Lee, H. Kim, and K. Kim, "Strong proxy signgture and its applications," in *Proceedings of SCIS'01*, pp. 603-608, 2001.

[9] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," in *Proceedings of the ACISP'01*, pp. 474-486, 2001.

[10] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," in *Proceedings of International Conference on Chinese Language Computing*, pp. 273-277, Illinois, USA, July 2000.

[11] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proceedings 3rd ACM Conference on Computer and Communications Security*, pp. 48-57, ACM Press, 1996.

[12] A. Nicolosi, M. Krohn, Y. Dodis, and D. Mazieres, "Proactive two-party signatures for user authentication," in *Proceedings of 10th Annual Network and Distributed System Security Symposium (NDSS'03)*, 2003.

[13] H. U. Park and I. Y. Lee, "A digital nominative proxy signature scheme for mobile communication," in *Proceedings of the International Conference on Information and Communications Security (ICICS'01)*, LNCS 2229, pp. 451-455, Springer-Verlag, 2001.

[14] D. Pointcheval and J.Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, 2000.

[15] S. H Seo and S. H. Lee, "New nominative proxy signature scheme for mobile communication," in *Proceedings of the Security and Protection of Information (SPI'03)*, ISBN: 80-85960-50-8, pp. 149-154, 2003.

[16] K. Shum and V. K. Wei, "A strong proxy signature scheme with proxy signer privacy protection," in *Eleventh IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprise*, 2002.

[17] H. M. Sun, "An efficient nonrepudiable threshold proxy signatures with known signers," *Computer Communications*, vol. 22, no. 8, pp. 717-722, 1999.

[18] H. M. Sun and B. T. Hsieh, *On the Security of some Proxy Signature Scheme*, Cryptology ePrint Archive, Report 2003/068, 2003.

[19] H. Sun, N. Y. Lee, and T. Hwang, "Threshold proxy signatures," *IEE Proceedings - Computes and Digital Technique*, vol. 146, pp. 259-263, 1999.

[20] Z. W. Tan, Z. J. Liu, and C. M. Tang, "Proxy blind signature scheme based on DLP," *Journal of Software*, vol. 14, pp. 1931-1935, 2003.

[21] G. L. Wang, "Designated-verifier proxy signatures for e-commerce," in *IEEE 2004 International Conference on Multimedia and Expo (ICME'04)*, Taipei, June 2004.

[22] H. X Wang and J. Pieprzyk, "Efficient One-time proxy signatures," in *Asiacrypt'03*, pp. 507-522, Springer-Verlag, 2003.

[23] K. Zhang, "Threshold proxy signature schemes," in *1997 Information Security Workshop*, pp. 191-197, Japan, 1997.

Zuo-Wen Tan is an assistant professor at Jiangxi University of Finance & Economics. He received his Ph.D. from Institute of Systems Science, AMSS, CAS in June 2005 and Master degrees from Xiangtan University in June 2002. His research interests include information security and cryptography.