Volume: 02, Issue: 01, Pages: 411-418 (2010)

A Secure Nominative Proxy Signature Scheme for Distributed Shared Object Systems

I. A. Ismail
Department of Information Technology, Faculty of Computers and Informatics,
Zagazig University, Zagazig, Egypt.
S. F. El-Zoghdy
Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Egypt
Email: elzoghdy@yahoo.com
A.A. Abdo
Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Egypt
Email: azza2asd@yahoo.com

-----ABSTRACT-----
Digital signature scheme is an important research topic in cryptography. An ordinary digital signature scheme allows a signer to create signatures of documents and the generated signatures can be verified by any person. A proxy signature scheme, a variation of ordinary digital signature scheme, enables a proxy signer to sign messages on behalf of the original signer. To be used in different applications, many proxy signatures schemes were proposed. Among them, Soe and Lee nominative Proxy Signature scheme, and Jianhong Zhang, Jianhong Zou, and Yumin Wang nominative Proxy Signature scheme for mobile communication. The authors of these schemes argued that their schemes satisfies the following security requirements: user anonymity, authentication and non-repudiation. However, in this paper, we show that their schemes do not satisfy the non-repudiation among their security requirements. And then we propose a new nominative proxy signature scheme that solves the weakness of their schemes. Unlike their schemes, the proposed scheme provides a non-repudiation property and moreover it is more secure than their schemes.

Keywords : Nominative Signature, Proxy Signature, Digital Signature, Cryptanalysis.

Date of Submission: January 15, 2010 Date of Acceptance: May 20, 2010

I. 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 this problem, S. Kim, S. Park and D. Won introduced a new type of signature, nominative signature [6, 8]. 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 merchants signature. On the other hand, the company must prevent the customer from distributing the digital product to others.

A proxy signature scheme, a variation of ordinary digital signature scheme, allows an entity, called the designator or original signer, to delegate another entity, called a proxy signer, to sign messages on its behalf, in case of say, temporal absence, lack of time or computational power, etc. The delegated proxy signer can compute a proxy signature that can be verified by anyone with access to the original signers certified public key [16]. Proxy signatures have found numerous practical applications, particularly in distributed computing where delegation of rights is quite common. Examples discussed in the literature include distributed systems [17, 18], Grid computing [19], mobile agent applications [20, 21], distributed shared object systems [22], global distribution networks [23], and mobile communications [1]. The proxy signature primitive and the first efficient solution were introduced by Mambo, Usuda and Okamoto [7]. Since then proxy signature schemes have enjoyed a considerable amount of interest from the cryptographic research community. New security considerations and constructions have been proposed, old schemes have been broken, followed by more constructions (e.g., [1, 2, 3, 15, 16, 28]). Furthermore, many extensions of the basic proxy signature primitive have been considered. These include threshold proxy signatures [24, 25], blind proxy signatures [26], proxy signatures with warrant recovery [27], nominative proxy signatures [3], and one-time proxy signatures [20].

The nominative proxy signature is a useful tool in mobile communication environment because it provides mobile users anonymity through the nominative signature and decreases the mobile users computational cost through the proxy signature. Recently, Park and Lee introduced the concept of nominative proxy signature, and proposed a digital nominative proxy signature for mobile communication [1]. In 2003, Seo and Lee claimed that the Park-Lee scheme is insecure and proposed a new digital nominative proxy signature for mobile communication (**Soe-Lee scheme**) [3]. In 2005, Jianhong Zhang, Jianhong Zou, and Yumin Wang argued that Seo and Lee scheme is insecure and they proposed two modified nominative proxy signature schemes for mobile communication (**Z-Wang scheme**) [13].

In this paper, we first analyze Soe-Lee [3], and Z-Wang [13] nominative proxy signature Schemes, then we show that these schemes do not satisfy the non-repudiation. Next a new nominative Proxy Signature scheme that provides the non-repudiation is proposed. It doesn't require a secure channel between the original signer and the proxy signer.

The rest of this paper is organized as follows. In Section II, we briefly review some properties of the nominative proxy signature schemes. In Section III, we recall Soe-Lee's nominative proxy signature scheme and gives its cryptanalysis. In section IV, we present Jianhong Zhang, Jianhong Zou, and Yumin Wang nominative proxy signature scheme and present its cryptanalysis. In Section V, we present the proposed nominative proxy signature scheme and analyze its security. Finally, section VI summarizes this paper.

II. REVIEW ON NOMINATIVE PROXY SIGNATURE (NPS)

The nominative proxy signature scheme(NPS) is a method in which the designated proxy signer generates the nominative signature and transmits it to a verifier, instead of the original signer. An original-nominative proxy signature scheme should satisfy the following requirements [6, 7]:

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.

NPS 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). Since a mobile user can designate a proxy agent as the proxy signer, the mobile users computational cost for signing can be decreased by the proxy agent, hence, the NPS schemes are useful methods in mobile communication environment.

III. REVIEW ON SOE-LEE'S NPS

In this section, we will recall Soe-Lee's NPS [3]. This scheme involves three entities the sender A, Proxy signer B, and the receiver C. The system parameters are:

- p, q: two prime large numbers, $q/(p-1)$.
- g: an element of Z_p^* its order is q.
- x_A, x_B, x_C: Original signer A's private key, the proxy signer B's secret key, and the receiver C's secret key respectively.
- $Y_A = g^{x_A} (\text{mod } p), Y_B = g^{x_B} (\text{mod } p), Y_C = g^{x_C}$: A's, B's, and C's are public keys respectively.
- $H(.)$: one way hash function.
- $||$: which denote the concatenation of string.
- T: Time stamp of the message.

The same parameters are used through this paper.

A. *Description Of Soe-Lee's NPS Scheme*

1. **Proxy Generation:** A chooses a random $k \in_R Z_q - \{0\}$, then computes:
   $r = g^k (\text{mod } p)$,
   $S_A = x_a . H(M_w || r || T) + k.r (\text{mod } q)$
2. **Proxy delivery:** A gives the pair (M_w, T, r, s_A) to the proxy B in a secure manner.
3. **Proxy verification and alternation:** B checks $g^{S_A} = y_A^{H(M_w||r||T)} r^r (\text{mod } p)$. If it is correct, B accepts A, otherwise rejects the signature. B generates the proxy signature by $S_p = S_A + x_B H(M_w||r||T||y_c) (\text{mod } q)$. S_p and y_p are the secret and public proxy signature key, respectively.
4. **NPS generation:** B chooses $k_1, k_2 \in_R Z_q$ at random then computes:
   $R = g^{k_1 - k_2} (\text{ mod } p)$
   $Z = y_C^{k_1} (\text{ mod } p)$
   $e = H(M||Mw|| T||y_c||R||Z)$,
   $S = k_2 - eS_p (\text{mod } q)$
5. **NPS delivery:** B sends $(M, T, r, R, Z, M_W, y_c, S)$ to C
6. **Verification of Proxy Signature delivery:**
   The verifier C first checks if message M signed conforms to the warrant M_w, then computes the proxy signature public key y_p
   $y_p = y_A^{H(M_w||r||T)} (r.y_B)^r (\text{mod } p)$,
   $e = H(M_w || T || y_c || R || z)$.
   Then C verifies the NPS on a message M by checking $(g^s . y_p^e . R)^{x_c} = Z(\text{ mod } p)$.

B. *Cryptanalysis Of Soe-Lee's Scheme*

Although this scheme tries to solve the weakness of Park-Lee's scheme [1]. It still has the same weakness as Park-Lee's scheme (i.e., the scheme still does not provide non-repudiation).

Volume: 02, Issue: 01, Pages: 411-418 (2010)

[The Attack Scenario in case of a malicious original signer]

1. malicious signer A' chooses a random $k \in_R Z_q$ then computes:

   $r = y_B^{-1}.g^k \pmod p$,

   $d = H(M_w \| r \| T)$,

   $S_A = x_a.d + k.r \pmod q$.
2. A' puts $S_p = S_A$, and then chooses $k_1 \in_R Z_q$, and then computes:

   $R = g^{k_1} \pmod p$,

   $Z = y^{k_1}{}_C \pmod p$,

   $e = H(M \| M_w \| y_C \| R \| Z)$,

   $S = -e.S_p \pmod q$.
3. A' sends $(M, M_w, T, y_c, r, R, Z, S)$ as a valid Proxy Signature on a message M to C.
4. **Verification:** The verifier C computes

   $d = H(M_w \| M \| T)$,

   $e = H(M \| M_w \| y_C \| R \| Z)$,

   $y_p = y_A^d.(y_B.r)^r \pmod p$.

   The value of y_p is correct since:

$$y_p = g^{S_p} = g^{S_A}$$
$$= g^{x_a.d+k.r}$$
$$= g^{x_a.d}.g^{k.r}$$
$$= y_A^d.(y_B.r)^r$$

And then, it verifies the nominative proxy signature by checking a congruence $(g^s.y_p^e.R)^{x_c} = Z \pmod p$.

Which is true since:

$$(g^S.y_p^e.R)^{x_c} = (g^{k_2 - e.S_p}.g^{e.S_p}.g^{k_1 - k_2})^{x_c}$$
$$= (g^{k_1})^{x_c}$$
$$= y_c^{k_1}$$
$$= Z$$

Example 1:

Let q = 579533 is a prime number and p = 15067859 , and $p = 26 \times q + 1$ is a prime number, hence since 11 is a primitive element in Z_p, so we can take $g \equiv 11^{26} \bmod 15067859 \equiv 13905710$, g is a q root of 1 modulo p, i.e. $g^q \bmod p \equiv 1$. Suppose dishonest signer A' selects k = 50, then he can computes

$r \equiv g^k \pmod p \equiv (13905710)^{50} \pmod{15067859}$

$\equiv 14678721$.

Let $H(m_w \| T \| r) = 96$, then

$S_A \equiv x_a.H(M_w \| T \| r) + k.r \pmod q$

$\equiv (333 \times 96) + 50 \times 14678721 \pmod{579533}$

$\equiv 257928$

Signing phase: B chooses $k_1 = 90,\ k_2 = 55$, and then computes

$R \equiv g^{k_2 - k_1} \pmod p$

$\equiv (13905710)^{90-55} \pmod{15067859}$,

$\equiv (13905710)^{35} \pmod{15067859}$,

$\equiv 13819566$,

$Z \equiv y_C^{k_1} \pmod p$

$\equiv 14321287^{90} \pmod{15067859}$

$\equiv 11628803$

$S_p \equiv S_A \equiv 257928$

let $e \equiv H(M \| M_w \| T \| y_{C|} | r \| R \| Z) \equiv 98$.

Then A' calculates $S \equiv (k_2 - S_p.e) \pmod q$

$\equiv 55 - 257928 \times 98 \pmod{579533} \equiv 222563$.

The nominative Proxy Signature on a message M is (M, M_w, T, e, r, S). A' sends (M, M_w, T, e, r, S) to C.

Verification: The verifier C Computes:

$y_p \equiv y_A^d.(y_B.r)^r$

$\equiv g^{S_A} \pmod p$

$\equiv 13905710^{257928}$

$e \equiv H(M \| M_w \| T \| y_C \| r \| R \| Z)$

$\equiv 98$

and checks if $(r.y_B{}^r)^{r.e} = (r.y_B{}^r)^{(p-1).e} = 1$.

Then C accepts the signature.

IV. Review Of Z-wang scheme

Jianhong Zhang, Jianhong Zou, and Yumin Wang introduced a cryptanalysis of Seo-Lee scheme, and proposed two modified signature schemes [13] to solve the weakness of Seo-Lee's scheme. In this section, we recall one of them and break it. The system parameters as in Soe-Lee's:

A. Description Of Z-wang Scheme

1. **Proxy Generation:** A chooses a random $k \in_R Z_q - \{0\}$ then computes

   $r = g^k \pmod p$,

   $S_A = x_a.H(M_w \| r \| T) + k.r \pmod q$.
2. **Proxy delivery:** A sends (M_w, T, r, s_A) to the proxy B in a secure manner.
3. **Proxy Verification and alternation:** B checks $g^{S_A} = y_A{}^{H(M_w\|r\|T)} r^r \pmod p$. If it is correct, B accepts A. B generates the proxy signature by $S_p = S_A + x_B.r^2 \pmod q$.
4. **NPS generation:** B chooses $k_1, k_2 \in_R Z_q$ at random and computes:

$$R = g^{k_1 - k_2} \pmod{p}$$
$$Z = y_C^{k_1} \pmod{p}$$
$$e = H(M \parallel M_w \parallel y_C \parallel R \parallel Z),$$
$$S = k_2 - eS_p \pmod{q}.$$

5. **NPS delivery:** *B* sends $(M, T, r, R, Z, M_w, y_c, S)$ to *C*.
6. **Verification of Proxy Signature delivery:** The verifier *C* first checks if message *M* signed conforms to the warrant M_w, then computes the proxy signature public key y_p

$$y_p = y_A^{H(M_w \| r \| T)} (r.y_B{}^r)^r \pmod{p}$$
$$e = H(M_w \parallel T \parallel y_c \parallel R \parallel z).$$

Then *C* verifies the NPS on a message *M* by Checking $(g^s.y_p^e.R)^{x_c} = Z \pmod{p}$.

B. Cryptanalysis Of Z-wang Scheme

Although Z-Wnag scheme tries to solve the weakness as Seo-Lee's scheme. It still has the same weakness as Park-Lee's scheme (i.e., the scheme still does not provide non-repudiation).

[The Attack Scenario in case of malicious original signer]

1. A' chooses $k_1, k_2 \in_R Z_q$ and then computes

$$R = g^{K_1 - k_2} \pmod{p},$$
$$Z = y_C^{k_1} \pmod{p},$$
$$e = H(M \parallel M_w \parallel y_C \parallel R \parallel Z).$$

For the value of *e*, any of the following three cases may occur:

Case 1: *e* is even, and $\gcd(e, p-1) = 2$, put

$$r = \frac{(p-1)}{2}, \text{ then } (r.y_B{}^r)^{r.e} = (r.y_B{}^r)^{\frac{(p-1)}{2}.e}$$

$= (r.y_B{}^r)^{(p-1).\frac{e}{2}} = 1$ since $\frac{e}{2}$ is an integer number (Fermat's Little Theorem since for any integer $a \succ 0$ then $a^{p-1} \bmod p = 1$)

Case 2: *e* is even or odd, and $\gcd(e, p-1) = a \geq 2$, put

$$r = \frac{(p-1)}{a}, \text{ then } (r.y_B{}^r)^{r.e} = (r.y_B{}^r)^{\frac{(p-1)}{a}.e}$$

$= (r.y_B{}^r)^{(p-1).\frac{e}{a}} = 1$ since $\frac{a}{e}$ is integer number.

Case 3: *e* is odd, and $\gcd(e, p-1) = 1$, , put $r = (p-1)$, then $(r.y_B{}^r)^{r.e} = (r.y_B{}^r)^{(p-1).e} = 1$.

2. A' computes
$$d = H(M_w \parallel r \parallel T),$$
$$S_p = x_a.d, \; S = k_2 - e.S_p$$
3. A' sends $(M, M_w, T, y_c, r, R, Z, S)$ as a valid Proxy Signature on a message *M* to *C*.
4. **Verification:** The verifier *C* computes
$$d = H(M_w \parallel r \parallel T),$$
$$e = H(M \parallel M_w \parallel y_C \parallel R \parallel Z),$$
$$yp = y_A^d.(y_B.r)^r (\bmod p).$$

And then, it verifies the nominative proxy signature by checking a congruence $(g^s.y_p^e.R)^{x_c} = Z$.

Which is true since:

$$(g^S.y_p^e.R)^{x_c} = (g^{k_2 - e.S_p}.y_A^{d.e} (r.y_B{}^r)^{r.e}.g^{k_1 - k_2})^{x_c}$$
$$= (g^{k_2 - e.x_a.d}.y_A^{d.e}.1.g^{k_1 - k_2})^{x_c}$$
$$= (g^{k_1})^{x_c} = y_c^{k_1} = Z.$$

Example 2 *:*
Suppose the vales of p, q, g are as example 1.
Signing phase: A′ chooses $k_1 = 100, k_2 = 55$, and then computes

$$R \equiv g^{k_1 - k_2} \pmod{p}$$
$$\equiv (13905710)^{200-100} \bmod 15067859$$
$$\equiv (13905710)^{100} \bmod 15067859$$
$$\equiv 11467953$$
$$Z \equiv y_C^{k_1} \pmod{p}$$
$$\equiv 14321287^{200} \bmod 15067859$$
$$\equiv 1275429$$

let $e \equiv H(M \parallel M_w \parallel T \parallel y_C \parallel R \parallel Z) \equiv 13.$

Then **Case 2** is satisfied since
$$\gcd(e, p-1) = \gcd(13, 15067858) = 13 \succ 2, \text{ put}$$
$$r \equiv \frac{p-1}{r} \bmod p \equiv \frac{1506785}{13} \bmod 15067859$$
$$\equiv 1159066,$$

then

$$(y_B^r.r)^{r.e} \pmod{p} \equiv$$
$$((3345178^{3345178} \times 3345178)^{3345178})^{13} \bmod p \equiv 1$$
$$S_p \equiv x_A \times H(M_w \parallel r \parallel T) \bmod q$$
$$\equiv 111 \times 96 \pmod{579533}$$
$$S \equiv (k_2 - S_p.e) \equiv (100 - 13 \times 10656) \bmod q$$
$$\equiv 441105.$$

The nominative Proxy Signature on a message *M* is (M, M_w, T, e, r, S) to *C*.

Verification: The verifier *C* Computes:

$$y_p \equiv y_A^d.(y_B.r)^r \pmod{15067859}.$$
$$\equiv 14565411^{96} \times (3345178^{3345178} \times 3345178)^{3345178}$$
$$\pmod{p} \equiv 12062275$$

and checks if

$$(g^S.y_p^e.R)^{x_c} \pmod{p} \equiv (13905710^{441105} \times 1275429^{13}$$
$$\times 11467953)^{333} \pmod{p} \equiv 1275429 \equiv Z.$$

Then *C* accepts the signature.

V. PROPOSED NOMINATIVE PROXY SIGNATURE SCHEME

In this section, we present the proposed nominative proxy signature scheme in details. The system parameters as in Soe-Lee's.

A. Description Of the Proposed Nominative Proxy Signature scheme

1. **Proxy phase:**

(a) **Commission generation:** The original signer *A* generates a warrant m_w, which records the delegations, limits of authority, the identities of the original signer, the proxy signer, and the valid period of delegation. *A* chooses a random $K \in Zq$, then computes

$$r = g^k \pmod p. \quad (1)$$

$$S_A = x_a.H(M_w \| T \| r) + k.r \pmod q. \quad (2)$$

(b) **Proxy delivery:** *A* sends (M_w, T, r, s_A) to the proxy *B* in a secure manner.

(c) **Proxy verification:** After the proxy *B* receives the delegation key and warrant, it checks

$$g^{S_A} = r^r.y_a^{H(M_w\|T\|r)} \pmod p. \quad (3)$$

If it is correct, *B* accepts *A*, and then computes the proxy signature key as follows:

$$S_p = S_A + x_B.r.H(M_w \| T \| r) \pmod q. \quad (4)$$

2. **Nominative proxy signing phase:** To generate the proxy signature on a message *M*, *B* chooses k_1, and then computes the values of *Z*, and *R* as in Seo-Lee, the values of *e* and *S* as follows:

$$R = g^{k_2} \pmod p,$$

$$Z = y_c^{K_1} \pmod p,$$

$$e = H(M \| M_w \| T \| y_c \| r \| R \| Z),$$

$$S = \frac{k_1}{(k_2 + S_P.e)}$$

After that *B* sends the nominative Proxy Signature on a message *M* in the form (M, M_w, T, r, r', S) to *C*.

3. **Nominative proxy signature verification phase:** The verifier *C* computes :

$$y_p = r^r(y_A y_B{}^r)^{H(M_w\|T\|r)} \pmod p, \quad (5)$$

$$e = H(M_w, T, r), \quad (6)$$

$$K = (g^{r'}.y_p)^{S.x_c} \pmod p. \quad (7)$$

And then, it verifies the nominative proxy signature by checking a congruence $(R.y_p^e)^{S.x_c} \pmod p = Z$ which is true since:

$$(R.y_p^e)^{S.x_c} = \{g^{k_2}.g^{e.S_p}\}^{S.x_c}$$
$$= g^{\{(k_2+e.S_p).S\}.x_c}$$
$$= g^{k_1.x_c}$$
$$= Z$$

Then *B* sends the nominative proxy signature on a message *M* in the form $(M, M_w, T, e, r, R, Z, S)$ to *C*.

4. **Nominative proxy confirmation phase:** The nominee *C* (receiver) can proof to a third party (verifier) *V* the validity of the signature. The nominee *C* can proves that $(R.y_p^e)^{S.x_c} \pmod p = Z$, and $g^{x_c} = y_C \pmod p$ in a zero knowledge protocol manner, using Schanorr's Zero-knowledge confirmation protocol [6], we can construct a nominative signature as follows.

   1. The third party (verifier *A*) chooses randomly $a, b \in_R [1, q]$, and computes
      $$ch = (y_A^e.R)^a.g^b \pmod p.$$

   Give *ch* to the nominee *C*.

   2. The nominee *B* chooses randomly $a, b \in_R [1, q]$, and computes:
      $$h_1 = ch.g^t \pmod p)$$
      $$h_2 = h_1^{x_c} \pmod p)$$

   Give *h1* and *h2* to the third party.

   3. The third party sends *a* and *b* to the nominee.
   4. The nominee *C* verifies that
      $$ch = (y_A^e.R)^a.g^b \pmod p)$$

   If correct *C* gives t to the third party.

   5. The third party verifies that
      $$h_1 = (y_A^e.R)^a.g^{b+t} \pmod p)$$
      $$h_2 = Z^a.y_C^{b+t} \pmod p)$$

Example 3:

Suppose the vales of p, q, g are as example 1. Suppose Alice select k = 50, then She can compute

$$r \equiv g^k \pmod p \equiv (13905710)^{50} \pmod{15067859}$$
$$\equiv 14678721.$$

Let $H(m_w \| T \| r) = 96$, then

$$S_A \equiv x_a.H(M_w \| T \| r) + k.r \pmod q$$
$$\equiv (333 \times 96) + 50 \times 14678721 \pmod{579533}$$
$$\equiv 257928.$$

Alice sends $(M_w, T, r, sA) = (M_w, T, 14678721, 257928)$ to the proxy *B* in a secure manner. The proxy ensures that:

$$g^{S_A} \equiv r^r.y_a^{H(M_w\|T\|r)} \pmod p).$$

After that, he begins to generate the signature key:

$$S_p \equiv S_A + x_B.r.H(M_w \| T \| r) \pmod q$$
$$\equiv (257928) + (121 \times 14678721 \times 96) \pmod{579533}$$
$$\equiv 399936.$$

Signing phase: *B* chooses $k_1 = 51$, $k_2 = 53$, and then computes

$$R \equiv g^{k_2} \pmod p \equiv (13905710)^{53} \pmod{15067859}$$
$$\equiv 6442716$$
$$Z \equiv y_C^{k_1} \pmod p \equiv 14321287^{51} \pmod{15067859}$$
$$\equiv 6145841$$

Let $e \equiv H(M \parallel M_w \parallel T \parallel y_C \parallel r \parallel R \parallel Z) \equiv 98$.
Then *B* calculates

$$S \equiv \frac{k_1}{(k_2 + S_p.e)} \pmod q$$
$$\equiv 51 \times (53 + 399936 \times 98)^{-1} \pmod{579533}$$
$$\equiv 47004.$$

The nominative Proxy Signature on a message *M* is (M, M_w, T, e, r, S) to *C*.

The verification: The verifier *C* Computes:

$$y_p \equiv r^r (y_A y_B{}^r)^{H(M_w \parallel T \parallel r)} \pmod p$$
$$\equiv 14678721^{14678721} \times (14565411 \times 3345178^{14678721})^{96}$$
$$\pmod{15067859} \equiv 14603766$$
$$e \equiv H(M \parallel M_w \parallel T \parallel y_C \parallel r \parallel R \parallel Z)$$

and checks if

$$(R.y_p^e)^{S.x_c} \pmod p \equiv (6442716 \times 14603766)^{478004 \times 333}$$
$$\pmod{15067859} \equiv 6145841 \equiv Z.$$

Then *C* accepts the signature.

B. Analysis of the Proposed Scheme

Anyone can verify the validity of the proxy signature. Obviously, he can distinguish easily the proxy's signature from normal signature. Through the valid proxy signature, the verifier can confirm that the signature of the message has been entitled by the original. This occurs because during the verification, the verifier must use the originals public key. Also the proxy cannot repudiate the signature. The scheme offers non-repudiation property.

Theorem 1: *The proxy cannot allege his own signature.*

If the proxy tries to forge a proxy signature, he must obtain the secret key x_a of the original from equation 2 or choose *s* and *r* satisfying equation 3. In equation 2, since k is selected randomly, If he first chooses S_A and then tries to find r, he is trying to solve equation 3 for the unknown r. This problem has no feasible solution. From equation 4, we know that only the proxy signer holds his secret proxy signature key x_B. Anyone else (even the original) cannot obtain the key and impersonate the proxy.

Theorem 2: no one else (even the original) can impersonate the proxy and forge his proxy signature.

If anyone tries to allege the proxy signature on behalf of *A* by selecting a random k_1, and then computes r', and selecting S_p, he needs to compute *S*, but he can't, because he does not have the secret key x_B.

Theorem 3: The verifier can't forge the signature

If he tries to do that, he needs first to compute $r' = H(y_c^{k_1} k_1 \parallel M)$ by selecting any random k_1, but he lies in the discrete logarithm problem which satisfy equation 7.

VI. CONCLUSION

In this paper, we first analyze Soe-Lee, and Z-Wang nominative proxy signature Schemes mobile communication, and show that these schemes do not satisfy the non-repudiation. Then we proposed a new NPS scheme that solves the weakness of their schemes. Unlike their schemes the proposed scheme provides a non-repudiation property and moreover, the proposed scheme becomes more secure than the Nominative Proxy Signature schemes of Soe-Lee, and Z-Wang.

REFERENCES

[1] Park, H.U, and I. Y. Lee, A digital Nominative Proxy Signature Scheme for Mobile Communication, *in Proc. international conference on information and communications security (ICICS'01)*, LNCS 2229, pp. 451-455, Springer-Verlag, 2001.

[2] Seo, Z.W.Tan, and S.H. Lee, Improvement on Nominative Proxy Signature Schemes , *in Proceeding of the International Journal of Network Security (INS)*, Vol.7, No.2, PP.175-180,Sep.2008.

[3] Seo S.H, and S.H. Lee, New Nominative Proxy Signature Scheme for mobile communication, *in Proceeding of the Security and Protection of Information (SPI'03),* pp. 149-154, springer-verlag, 2003.

[4] Herreweghen, E. Van , Secure anonymous signature-based transactions. In ESORICS 00: Proc. of the 6th European Symposium on Research in Computer Security, pages 55-71. Springer-Verlag, 2000. LNCS 1895.

[5] Yang, G. , D. Wong, and X. Deng. Efficient anonymous roaming and its security analysis In Proc. of the 3rd International Conference on Applied Cryptography and Network Security (ACNS 2005), pages 334-349. Springer-Verlag, 2005. LNCS 3531.

[6] Kim, S., S. Park, and D.Won, Zero-Knowledge Nominative Signatures, in Proc. of Pragocrypt96, International Conference on the Theory and Applications of Cryptology, pp.380-392, 1996.

[7] Mambo, M., K.Usuda, and E.Okamoto, Proxy signatures: Delegation of the Power to Sign Messages, in IEICE Trans. Fundamentals, vol.E79-A, no.9, pp.1338-1354, 1996.

[8] Kim, S., S. Park, and D. Won, Proxy Signatures, revisited, ICICS97,LNCS1334, pp. 223-232, Springer-Verlag, 1997.

[9] Lee, B. , H. Kim, and K. Kim, Strong proxy signature and its applications, in Proceedings of SCIS01, pp. 603-608, 2001.

[10] Lee, B. , H. Kim, and K. Kim, Secure mobile agent using strong non-designated proxy signature in Proceedings of the ACISP01, pp. 474-486, 2001.

[11] Kim. S. J. , S. J. Park, D. H. Won, Nominative signatures in Proceedings of the ICEIC95, pp. 68-71, 1995.

[12] Dai, J. , X. Wang, and J. Dong, Designated receiver proxy signature Scheme, Journal of Zhejiang university (Engineering Science), vol.38, no.11,PP.1422-1425,2004.

[13] Jianhong Zhang, Jiancheng zou, Yumin wang, Two Modified Nominative Proxy Signature schemes for Mobile Communication, Proceedings of 2005 IEEE Networking, Sensing and Control. pp 435-437, Tucson, Arizona, USA.

[14] M. Bellare and G. Neven Multi-signatures in the plain public-key model and a general forking lemma. In CCS06, pages 390-399. ACM Press, 2006.

[15] G. Fuchsbauer and D. Pointcheval. Anonymous consecutive delegation of signing rights: Unifying group and proxy signatures. Cryptology ePrint Archive, Report 2008/037, 2008.

[16] A.Boldyreva, A. Palacio and B. Warinschi. Secure Proxy Signature Schemes for Delegation of Signing Rights. Cryptology ePrint Archive, Report 2003/096, 2003.

[17] B. C. Neuman. Proxy based authorization and accounting for distributed systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283-291, 1993.

[18] V. Varadharajan, P. Allen, and S. Black. An analysis of the proxy problem in distributed systems. In Proceedings of 1991 IEEE Computer Society Symposium on Research in Security and Privacy, pages 255-275, 1991.

[19] Erin Cody, Raj Sharman, Raghav H. Rao, Shambhu Upadhyaya Security in grid computing: A review and synthesis, Decision Support Systems, 44, p. 749-764, 2008.

[20] H. Kim, J. Baek, B. Lee, and K. Kim. Secret computation with secrets for mobile agent using one-time proxy signature. In Cryptography and Information Security 2001.

[21] B. Lee, H. Kim, and K. Kim. Strong proxy signature and its applications. In SCIS, 2001.

[22] J. Leiwo, C. Hanle, P.Homburg, and A. S. Tanenbaum. Disallowing unauthorized state changes of distributed shared objects. In SEC, pages 381-390, 2000.

[23] A. Bakker, M. Steen, and A. S. Tanenbaum. A law-abiding peer-to-peer network for free software distribution. In IEEE International Symposium on Network Computing and Applications (NCA01), 2001.

[24] J. Herranz and G. Saez. Revisiting fully distributed proxy signature schemes. Cryptology ePrint Archive, Report 2003/197., 2003

[25] H. M. Sun. An efficient non-repudiable threshold proxy signature scheme with known signers. Computer Communications, 22(8):717-722,1999.

[26] S. Lal and A. K. Awasthi. Proxy blind signature scheme. Cryptology ePrint Archive, Report 2003/072., 2003.

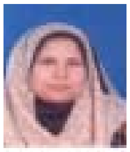
[27] S. Lal and A. K. Awasthi. A scheme for obtaining a warrant message from the digital proxy signatures. Cryptology ePrint Archive, Report 2003/073., 2003.

[28] N.R.Sunitha, and B.B.Amberker Proxy Signature Schemes for Controlled Delegation Journal of Information Assurance and Security, 2,P. 159-174, 2008

Authors Biography

Prof Ismael Amr Ismail Was born in Cairo, Egypt, in 1946. He received the BSc degree in pure Mathematics and physics Cairo university 1967. MSc degree for his work in computer science Cairo university in 1974. Ph. D. degree from Cairo university in 1976. Professor of computational math 1989. Dean of computer science Zagazige Univ. 1998-2006. Dean of computer science Missr Univ. 2006- to date. More than 102 international published papers. His research interests are in image processing, parallel computing, Security and Cryptography.

Dr. Said Fathy El-Zoghdy Was born in El-Menoufia, Egypt, in 1970. He received the BSc degree in pure Mathematics and Computer Sciences in 1993, and MSc degree for his work in computer science in 1997, all from the Faculty of Science, Menoufia, Shebin El-Koom, Egypt. In 2004, he received his Ph. D. in Computer Science from the Institute of Information Sciences and Electronics, University of Tsukuba, Japan. From 1994 to 1997, he was a demonstrator of computer science at the Faculty of Science, Menoufia University, Egypt. From December 1997 to March 2000, he was an assistant lecturer of computer science at the same place. From April 2000 to March 2004, he was a Ph. D. candidate at the Institute of Information Sciences and Electronics, University of Tsukuba, Japan., where he was conducting research on aspects of load balancing in distributed and parallel computer systems. From April 2004 to 2007, he worked as a lecturer of computer science, Faculty of Science, Menoufia University, Egypt. From 2007 until now, he is working as an assistant professor of computer science at the Faculty of Computers and Information Systems, Taif University, Kingdom of Saudi Arabia. His research interests are in load balancing in distributed/parallel systems, Grid computing, performance evaluation, network security and cryptography.



Azza Ahmed Abdo Ali Was born in Egypt, in 1982. She received the BSc degree in pure Mathematics and Computer Sciences in 2003, and MSc degree for her research in computer science in 2008, all from the Faculty of Science, Menoufia, Shebin El-Koom, Egypt. From 2005 to August 2008, she was a demonstrator of computer science at the Faculty of Science, Menoufia University, Egypt. From September 2008 to date, she is an assistant lecturer of computer science at the same place. Her research interests are in Image Processing, image Encryption, Symmetric Key Cryptography, and Multimedia Security.