Secure Undeniable Threshold Proxy Signature Scheme

Sattar J. Aboud
Department of Computer Science,
University of Bedfordshire,
UK

***Abstract*—The threshold proxy signature scheme allows the original signer to delegate a signature authority to the proxy group to cooperatively sign message on behalf of an original signer. In this paper, we propose a new scheme which includes the features and benefits of the RSA scheme. Also, we will evaluate the security of undeniable threshold proxy signature scheme with known signers. We find that the existing threshold proxy scheme is insecure against the original signer forgery. In this paper, we show the cryptanalysis of an existed scheme. Additional, we propose the secure, undeniable and known signers threshold proxy signature scheme which answers the drawback of an existed scheme. We also demonstrate that a threshold proxy signature suffers from a conspiracy of an original signer and a secret share dealer, that the scheme is commonly forgeable, and cannot offer undeniable. We claim that the proposed scheme offers the undeniable characteristic.**

Keywords—cryptography; digital signature; proxy signature; threshold proxy signature

I. INTRODUCTION

The proxy signature scheme is a method which allows original signer delegates his works to a designated person with a proxy signature key. The proxy signature key is generated by the original signer signature key which cannot be computed from the proxy signature key. The proxy signer can generate the proxy signature in a message on behalf of an original signer. Since Mambo *et al.* presented an idea of a proxy signature [1], various proxy signature schemes are suggested [2]. Based-on the type of delegation, a proxy signature is categorized into full delegation, partial delegation and delegation by warrant.

In full delegation, an original signer passes its private key as a proxy signature key to a proxy signer over a secure channel. In partial delegation, a proxy signer has the proxy signature key from a proxy signer secret key and a delegation key passed by an original singer. A delegation key is created by an original with the trap-door permutation of an original signer secret key. A proxy signature is dissimilar from an original and a proxy typical signature. In delegation by certificate, an original signer employs its typical signature to sign the warrant that records a kind of information delegated, an original signer and a proxy signer identities and a period of delegation. The signature of a warrant is a certificate that stops a passing of proxy power to a trusted authority.

The partial delegation can be altered into the partial delegation by warrant. A partial delegation by warrant can offer sufficient security and efficiency. For simplicity, we denote that a partial delegation by warrant a proxy signature. Mambo *et al*. proxy signature scheme satisfy a characteristic of no one except an original signer and a proxy signer can generate the valid proxy signature on behalf of an original signer. In 2001, Lee *et al.* [3] enhanced a security characteristic of a proxy signature by create a valid proxy signature and someone else, even an original signer, cannot create a valid proxy signature. So, for a valid proxy signature, a proxy signer cannot repudiate signed a message and an original signer cannot repudiate delegated a signing authority to a proxy signer. Namely, a proxy signature scheme has a security characteristic of undeniable.

The present proxy signature systems have two drawbacks. First, a declaration of the valid delegation in a warrant is not practical since a proxy signer can generate the proxy signature and claim that the signing was released through a delegation phase. Second, even if a signer key is compromised and the delegated rights are misused; and an original signer needs to revoke a delegation before his strategy, he can make anything. Therefore, a revocation of delegated rights is the important matter of a proxy signature system. To solve the above difficulties, some proxy signature systems have been suggested. Sun indicated that time-stamp proxy signature system and its enhancement [4]. But Sun scheme cannot solve the second drawback. Seo *et al.* [5] suggested a proxy signature system to solve a fast revocation difficulty. The scheme uses the third trusted entity, entitled Security Mediator which is the online partially trusted server.

II. RELATED WORKS

Based on a Shamir secret sharing scheme in 1979 [6].Zhang *et al*., in 1997 suggested a threshold proxy signature scheme [7]. In their scheme, the proxy signature key is shared among a subset of n proxy signers where at least t proxy signers can cooperatively sign documents on behalf of an original signer. To avoid argument regarding who is a proxy signer, Sun in 1999 [8] suggested the undeniable threshold proxy signature scheme with known signers. Sun scheme reduces Kim *et al.* scheme [2] drawbacks that a verifier is incapable to verify if a proxy group key is created by an authorized proxy group. In 2001 Hsu *et al*. [9] illustrated that Sun scheme is weak since any t proxy signers can get the private keys of other proxy signers. In 2003, Yang *et al.* [10] proposed an enhancement on Hsu *et al*. scheme. Yang *et al*. scheme is more efficient regarding the communication cost

and timing complexity. In 2004, Tzeng *et al.* [11] found that Hwang *et al*. scheme; malicious original signer can forge a threshold proxy signature without an agreement of the proxy signers. Tzeng *et al.* also built the undeniable threshold proxy signature scheme with known signers and claimed the suggested scheme enhanced a security of Hwang *et al*. scheme. In 2006, Yuan Yumin [12] introduced a threshold proxy signature scheme with non-repudiation and anonymity. Yuan Yumin claims that the scheme with any verifier can check if authors of a proxy signature belong to designated proxy group by the original signer, while outsiders cannot find the actual signers. In 2007, Qi Xie *et al*., [13] claims that their scheme made an improvement of undeniable_threshold multi-proxy threshold scheme with shared verification. In 2009, Hu and Zhang [14] presented a cryptanalysis and improvement of a threshold proxy signature scheme with undeniable. In 2012, Hwang *et al.,* proposed a scheme and claimed that its scheme eliminate the security leaks. But, in its scheme the improvement, a malicious original or proxy signer can forge a valid threshold proxy signature for any message by different ways. In this paper, we show the vulnerabilities of the Hwang *et al.,* scheme and proposed a new system that solves the existed problems.

The remainder of this paper is organized as follows. In Section 3, we will provide some notations and reconsider Pedersen threshold distributed key generation protocol [15]. In Section 4, we will analysis a security of Sun *et al*. threshold proxy signature scheme. In Section 5 we will describe the proposed scheme. Finally, conclusions are in Section 6.

III. PRELIMINARIES

In this Section, we will provide some notations used by this paper and also reconsider Pedersen threshold distributed key generation scheme.

A. Notaions Used

In this section, we provide the notations which are used by this paper.

p, q: Two large prime numbers where $q / p-1$.

g: Generator of Z_p^* its order is q

O: Original signer

$P_1, P_2, \ldots, P_n$: The n proxy signer

d_O: Private Key of an original singer O

e_O: Public key of an original signer O

d_i: Private Key of a proxy signer P_i

e_i: Public key of a proxy signer P_i

$h(.)$: Secure hash function.

$||$: Concatenation operation

id: The identity of the proxy signer

m_w: A warrant which records information delegated an original signer and proxy signer.

B. Penderson Threshold Distributed Key Generation Protocol

Pedersen threshold distributed key generation scheme contains n Feldman (t, n) verifiable secret sharing schemes [16]. Suppose $(P_1, P_2, \ldots, P_n)$ are n players. Pedersen scheme includes the following three stages.

1) Every player P_i arbitrarily selects a polynomial $f_i(z)$ over Z_q of degree $t-1$.

$$f_i(z) = a_{i0} + a_{i1} z + a_{i2} z^2 + \ldots + a_{i,t-1} z^{t-1} \quad (1)$$

P_i Transmit $b^{a_{i0}}, b^{a_{i1}}, \ldots, b^{a_{i,t-1}}$. Then finds and passes $f_i(j) \bmod q$ to P_j such that $j = 1,2,\ldots,n$ where $j \neq i$ in the secure channel.

2) Every P_j check a validity of a share $f_i(j) \bmod q$ by verifying for $i = 1,2,\ldots,n$,

$$b^{f_i(j)} = b^{a_{i0}} (b^{a_{i1}})^j (b^{a_{i2}})^{j^2} \ldots (b^{a_{i,t-1}})^{j^{t-1}} \bmod p$$

When all $f_i(j)$ are checked to be certified, P_j finds $x_j = \sum_{i=1}^{n} f_i(j) \bmod q$ as his share.

3) Assume $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots a_{t-1} z^{t-1} \bmod q$

$= \sum_{i=1}^{n} f_i(z) \bmod q$. Where, $a_r = \sum_{i=1}^{n} a_{ir} \bmod q$ for $0 \le r \le t-1$, and $x_i = f(i) \bmod q$ so $w = \sum_{i=1}^{n} x_i \bmod q$

when any t secret shares, say $w_1, w_2, \ldots, w_t$ are Lagrange interpolating polynomial:

$$w = f(0) = \sum_{i=1}^{i=t-1} s_i \prod_{j=1, j\neq i}^{t-1} \frac{0-j}{i-j} \bmod q \quad (2)$$

The validity of reconstructed private key w can be checked by the following formula holds: $b^w = \prod_{i=1}^{i=n} b^{a_{i0}} \bmod p$ (3)

IV. SIGNATURE OF THRESHOLD PROXY SIGNATURE SCHEME

We will describe two threshold proxy signature schemes which are follows:

Sun Scheme

The first scheme we will describe the Sun scheme as follows:

A. Description of Sum Scheme

First, we will describe Sun threshold proxy signature scheme as follows:

Secret Share Generation Phase

In this phase, a proxy group $(P_1, P_2, \ldots, P_n)$ should do the following:

1) Create a group of private and public key pair $(w, e_1) \in Z_q^* \times Z_p$.

1. Run Pedersen threshold distributed key generation protocol as described in Section 2.

2) Every player P_i *uses* $f_i(z) = d_i + a_{i0} + a_{i1}z + a_{i2}z^2 + \ldots + a_{i,t-1}z^{t-1}$

3) The private key shared by a proxy group is $w = \sum_{i=1}^{n} d_i$

4) The related public key is $e_i = \prod_{i=1}^{n} e_i \bmod p$.

5) Gets a secret key share $x_i = f(i) = \sum_{j=1}^{t} f_j(i) \bmod q$.

6) Declare $u_j = b^{v_j} \bmod p, j = 1,2,\ldots,t$.

Proxy Share Generation Phase

In this phase, an original signer O creates a proxy share as follows.

Step 1: Original Signer O

1) arbitrarily selects $r \in Z_q$

2) find $l = b^r \bmod p$

3) Compute proxy $k = d_O h(m_w \| l) + r \bmod q$.

4) Allocate a proxy key k between a proxy groups by implementing Feldman scheme.

5) Selects an arbitrarily polynomial of degree $t-1$ *:* $f^{-}(z) = k + g_1 z + g_2 z^2 + \ldots, + g_{t-1} z^{t-1} \bmod q$

6) Finds and privately passes $k_i = f^{'}(i) \bmod q$ *to a proxy signer* P_i *for* $i = 1,2,\ldots,n$

7) Declares (m_w, l) *and* $v_j = b^{g_j}\ (j = 1,2,\ldots,t-1)$

Step 2: Proxy Signer P_i

1) Accepts (k_i, m_w, l) *when a formula* $b^{k_i} = e_O^{h(m_w \| l)} l \prod_{j=1}^{t-1} v_j^{i^j} \bmod p$ *correct*

2) Find $k_i = k_i + x_i h(m_w \| l) \bmod q$ *as a proxy share.*

Proxy Signature Generation Phase

Suppose that $(P_1, P_2, \ldots, P_t)$ as an actual proxy group signs a document m as follows:

1) The t proxy signer runs Pedersen threshold distributed key generation protocol for sharing value $c_O = \sum_{i=1}^{t} c_{i,O}$ *using* $f_i^{''}(z) = (c_{i,O} + d_i) + c_{i,1}z + c_{i,2}z^2 + \ldots, + c_{i,t-1}z^{t-1} \bmod q$

2) Each P_i *for* $i = 1,2,\ldots,t$ *gets the public key* $y = b^{c_O} \bmod p$ *and a private arbitrary value share* $x_i^{'} = f^{''}(i) = \sum_{i=1}^{t} d_i + c_O + c_1 i + c_2 i^2 + \ldots + c_{t-1} i^{t-1} \bmod q$ *such that* $c_j = \sum_{i=1}^{t} c_{ij}$ *for* $1 \le j \le t-1$

3) Each, P_i *finds proxy signature share* $s_i = x_i y + k_i h(id \| m) \bmod q$

4) Pass s_i *to proxy signers* $P_j = (j = 1,2,\ldots,t, j \ne i)$ *in the secure channel.*

5) Each P_j *can check a validity of* s_i *by verifying when the following formula correct:*

$$b^{s_i} = \left[e \left(\prod_{j=1}^{t-1} c_j^{i^j} \right) \left(\prod_{j=1}^{t} e_j \right) \right]^e \left[(l_{e_O}^{h(m_w \| l)} \prod_{j=1}^{t-1} v_j^{i^j}) \left(e_1 \prod_{j=1}^{t-1} u_j^{i^j} \right)^{h(m_w \| l)} \right]^{h(id \| m)} \bmod p$$

6) Every proxy signer in actual proxy group can creates $s = f^{''}(0)e + \left[f(0) + f^{'}(0) \right] h(id \| m)$ *by a Lagrange interpolation formula to* s_i.

7) The proxy signature on m is (m, m_w, l, id, e, s).

Proxy Signature Verification Phase

The verifier can identify an original signer and an actual proxy signers from m_w, and id, and validate a proxy signature by verifying when

$$b^s = \left[l_{e_O}^{h(m_w \| l)} \prod_{i=1}^{n} e_i \right]^{h(id \| m)} \left(y \prod_{i=1}^{t} e_i \right)^y \bmod p \quad (4)$$

B. Cryptanalysis of Sun Threshold Proxy Signature Scheme

In this subsection, we illustrate that Sun scheme is weak against an original signer forgery. Since the malicious original signer can create the proxy signature on every document and claim that any t proxy signers can be actual proxy signers of a proxy signature. Assume a message m; an original signer O arbitrarily selects the proxy group (thus, O selects id).

1) Suppose that O imitates proxy signers $(P_1, P_2, \ldots, P_t)$.

2) Then O find s $l = (\prod_{i=1}^{t} e_i)^{-1} g^a \bmod p$ *where* $e = (\prod_{i=1}^{t} e_i)^{-1} b^v$, *such that* $a \in Z_q, v \in Z_q$.

3) Then, O finds:

$$s = (a + d_O h(m_w \| l)) h(id \| m) + ve \bmod q \quad (5)$$

4) So (m, m_w, l, id, e, s) *is the valid proxy signature on message m since*

$$b^s = b^{(a + d_O h(m_w \| l)) h(id \| m) + ve} \bmod p$$

$$= b^a b^{d_O h(m_w \| l) h(id \| m)} (b^v)^e \bmod p$$

$$= \left(l_{e_O}^{h(m_w \| l)} \prod_{i=1}^{n} e_i \right)^{h(id \| m)} (y \prod_{i=1}^{t} e_i)^y \bmod p$$

1.

C. The Vulnerability of Sun Scheme

With Sun (t, n) threshold proxy signature system, the verifier checks a validity of a proxy signature and recognizes the real signers. Though, in this paragraph we illustrate that a proxy signer private key is not protected. The $(n-1)$ proxy signers in a group of n can present their private keys to conspire a private key of a residue one. We so-call this attack a collusion attack.

In this attack, any $(n-1)$ proxy signers in a group of n participants can masquerade a rest one. For instance, suppose that (3,5) threshold proxy signature system. A proxy signer $p_1,...,p_4$ aims to get a private key of a proxy signer p_5. Then, we can masquerade the authorized proxy signer p_5 to sign the document m. Any three proxy signers of $p_1,...,p_4$ can find a_0 using Lagrange equation since $a_0 = \sum_{i=1}^{5} d_i \bmod p$. So, proxy signers $p_1,...,p_4$ can appear the private keys to conspire a private key d_5 of a proxy signer p_5. We can masquerade a proxy signer p_5 to create the authorized proxy signature.

In the same manner s_5, k_5 and $k_5^{'}$ is calculated by using Lagrange equation. In proxy signature issuing phase, we can masquerade p_5 to share the arbitrary number, and we can obtain the secret $s_5^{'}$. By holding $s_5^{'}$ and $k_5^{'}$, we can get γ_5 and post it to other proxy signers of a proxy group. Then T can be calculated and then, a proxy group can create the proxy signature (m, T, l, m_w, id) for document m.

In a verification phase, a verifier can check a validity of a proxy signature and find p_5 as real signer of a proxy group. Actually, p_5 has never signed a document m, but cannot repudiate. Thus, in Sun scheme, a private key x_i of a proxy signer p_i can be compromised by collusion attack and hacker can masquerade authorized proxy signer p_i to sign the document.

Hwang *et al.* Scheme

This is the second threshold proxy signature scheme we are going to describe which is the Hwang *et al*. scheme [17] is the same as Sun threshold proxy signature scheme.

D. Description of Hwang et al. Scheme

First, we will describe Hwang *et al.* threshold proxy signature scheme as follows:

Secret Share Generation Phase

In this phase, a proxy group should do the following:

1) Creates group of private and public key pair $(w, e_1) \in Z_q \times Z_p$ *as in Sun scheme.*
2) Finds $f_i(z) = d_i + a_{i0} + a_{i1}z + a_{i2}z^2 + ... + a_{i,t-1}z^{t-1}$.
3) The secret key shared by a proxy group is $w = \sum_{i=1}^{n} d_i$
4) The related public key is $e_i = \prod_{i=1}^{n} e_i \bmod p$.
5) Gets the secret key share $x_i = f(i) = \sum_{j=1}^{n} f_j(i) \bmod q$.
6) Declares $u_j = b^{a_j} \bmod p$ *with* $j = 0,1,2,..t-1$.

Proxy Share Generation Phase

In the phase, an original signer O creates a proxy share as follows:

Step 1: Original Signer O

1) Creates a proxy key $k = h(m_w \| l) d_0 + r \bmod q$.
2) Selects arbitrarily polynomial of degree $t-1$ *:* $f^{'}(z) = k + g_1 z + g_2 z^2 + ... + g_{t-1} z^{t-1} \bmod q$
3) Finds and secretly posts $k = f^{'}(i) \bmod q$ *to* P_i *for* $i = 1,2,...,n$.
4) Declares (m_w, l) *, and* $v_j = b^{g_j} \bmod p$ *for* $j = 1,2,...,t-1$

Step 2: Proxy Signer P_i

1) Uses $k = h(m_w \| l)$ *when the following formula holds.* $b^{k_i} = y_0^{h(m_w, l)} \cdot l \cdot \prod_{j=1}^{t-1} v_j^{i^j} \bmod p$.
2) Finds $k_{ij} = k_i + x_i \cdot h(m_w \| l) \bmod q$.

Proxy Signature Generation Phase

We suppose $(P_1, P_2, ..., P_t)$ are actual proxy group. So, the steps of this phase as follows:

1) Creates a secret random share $x_i^{'}$ *as in Sun scheme.*
2) Finds a single proxy signature $s_i = x_i^{'} e + k_i^{'} h(id \| m) \bmod q$
3) Posts s_i *to the proxy signers* $P_j (j = 1,2,...,t, j \neq i)$ *in the secure way.*
4) Checks a validity of s_i *by verifying when the following formula holds:*

$$\left[\left(l^{e_0^{h(m\|l)}} \prod_{j=1}^{t-1} v_j^{i^j} \right) \cdot \left(e_1 u_0 \prod_{j=1}^{t-1} u_j^{i^j} \right)^{h(m_w \| l)} \right]^{h(id\|m)} b^{s_i} = \left[e \left(\prod_{j=1}^{t-1} c_j^{i^j} \right) \left(\prod_{j=1}^{t} e_j \right) \right] \bmod p \quad (6)$$

5) Using a Lagrange interpolation equation with s_i *, every signer can create* $s = f^{''}(0)e + \left[f(0) + f^{'}(0) \right] h(id \| m)$.
6) A proxy signature on m *is* $(m, m_w, l, id, e, u_0, s)$.

Proxy Signature Verification Phase

1) Verify a validity of a proxy signature from the following formula:

$$b^s = \left[l u_0 e_0^{h(m_w \| l)} \prod_{i=1}^{n} e_i \right]^{h(id\|m)} \left(e \prod_{i=1}^{t} e_i \right)^{e} \bmod p \quad (7)$$

2) When the formula holds, a proxy signature $(m, m_w, l, id, e, u_0, s)$ *is valid.*

E. Cryptanalysis of Hwang et al. Scheme Threshold Proxy Signature Scheme

In this subsection, we illustrate that Hwang *et al*. scheme is insecure versus universally forgery. The hacker can impersonate an original signer to forge the proxy signature on a message. Provided a message, an original signer, and the proxy group $(P_1, P_2, ..., P_n)$, a hacker selects $(P_1, P_2, ..., P_t)$ as actual proxy signers. Then, a hacker selects four arbitrary integers $a, v, \gamma \in Z_q^*$ and $e \in Z_p^*$. Then a hacker finds

$$l = \left(\prod_{i=1}^{n} e_i \right)^{-1} b^a \bmod p \quad (8)$$

$$u_0 = (e_0^{h(m_w \| l)})^{-1} b^v \bmod p$$

$$s = (a + v) h(id \| m) + \gamma e \bmod q \quad (9)$$

Therefore, $(m, m_w, l, id, e, u_0, s)$ is the valid proxy signature on message m, it convinces the following verification formula:

$$b^s = b^{(a+v)h(id\|m)+\gamma e} \bmod p$$
$$= (b^a b^v)^{h(id\|m)} b^{\gamma e} \bmod p$$
$$= \left[lu_0 e_0^{h(m_w\|l)} \prod_{i=1}^{n} e_i \right]^{h(id\|m)} \left(e \prod_{i=1}^{t} e_i \right)^{e} \bmod p$$

V. The Proposed Scheme

The suggested scheme combines theta $\theta(n)$ and an elimination of a computation of inverse in RSA scheme if we calculate a value of Lagrange coefficient. Also, we suggest an equation to find a result of message warrant m_w. Suppose that $N_O < N_i (i = 1,2,\ldots,n)$.

A. The Proxy Sharing Phase

The steps of the proxy sharing phase are as follows:

Step 1: Proxy Generation

The original signer O must do the following:

1) Find a group proxy signing key $d_1 = d_O^{m_w} \bmod \theta(N_O)$
2) Find the proxy verification key $e_1 = e_O^{m_w} \bmod \theta(N_O)$
3) Compute $m_w = (P + T + r)^T \bmod \theta(N_O)$ *such that* P *is a validity period of proxy signature and* T *is a sum of identities of* $P_O = P_1, P_2, \ldots, P_n$
4) Declare $(m_w, e_1, (m_w, e_1)^{d_O} \bmod N_O$

Step 2*:* Proxy Sharing

The original signer O must do the following:

1) Choose $t-1$ *degree polynomial* $f(x) = d_1 + a_1 x + .. a_{t-1} x \bmod N_O$ *with* $a_1, a_2, \ldots, a_{t-1}$, *are an arbitrary integers.*
2) Compute a proxy singer P_i *partial proxy signing key* $k_i = f(i)$
3) Pass $((k_i)^{d_O} \bmod N_O, k_i)^{e_i} \bmod N_i$ *to proxy signer* P_i

Step3: Proxy Share Generation.

The proxy signer P_i must do the following:

1) Receive $((k_i)^{d_O} \bmod N_O, k_i)^{e_i} \bmod N_i$
2) Obtain $((k_i)^{d_O} \bmod N_O, k_i)$ *by his secret key* d_i
3) Verify a validity of k_i *and keeps it secret.*

B. The Proxy Signature Issuing Phase

Suppose that T indicate the group members including any t proxy signers who desire to create the proxy signature on a message m on behalf of P_O cooperatively.

Step 1: Proxy Signer P_i

Every proxy signer P_i uses a partial proxy signing key k_i to do the following:

1) Create a partial signature $s_i = m^{k_i} \bmod N_O$
2) Pass $((s_i, i)^{d_i} \bmod N_i, s_i$ *to a combiner.*

Step 2: The Combiner

The combiner must do the following:

1) Receive partial signature s_i *from* P_i
2) Check the validity of a partial proxy signature by verifying if $(s_i, i)^{d_i e_i} \bmod N_i = (s_i, i)$.
3) Find $v = \prod_{id_a, id_b \in T} id_a - id_b$ *such that* $a > b$
4) Find $\prod_{id_a, id_b \in T} (id_a - id_b) \prod_{i=1, i \neq j}^{t} \frac{id_j}{id_i - id_j}$ *where* $\prod_{id_a, id_b \in T} (id_a - id_b)$ *a factor of* $\prod_{i=1, i \neq j}^{t} (id_i - id_j)$. *Thus,* L_i *are integer and combiner required not calculating inverse of* $\prod_{j=1, j \neq i}^{t} (id_i - id_j)$.
5) Create a signature $s = \prod s_i^{L_i} \bmod N_O$
6) The result of proxy signature is (v, s).

C. The Proxy Signature Verification Phase

The steps of this phase are as follows:

1) A verifier can check a signature signed on behalf of an original signer by a formula $s^{e_1} = m^v \bmod N_O$
2) An original signer can distinguish a proxy signer from a signature by $s_i^{d_i e_i} \bmod N_i = s_i$
3) An original signer can trace proxy signers by e_i.

VI. Comparisons

We compare the running of five schemes, Hwang *et al.* [17], Kim *et al.*[2], Hwang *et al.*[11], Sun *et al* [8] and Hsu *et al* [9] with a performance of the proposed scheme. The proposed scheme is efficient and secure anti-disreputable conspiracy attacks. Table 1 shows a comparison of threshold proxy signature schemes relied on proxy needs every scheme.

TABLE I. 1 The Comparision between Existed Schemes and Proposed Scheme

Security Features	Name of the Scheme				
	Kim	***Hwang***	***Sun***	***Hsu***	***Proposed***
Proxy Protection	No	Yes	No	No	Yes
Unforgeability	Yes	Yes	No	No	Yes
undeniable	Yes	No	Yes	Yes	Yes
Known Signer	No	Yes	Yes	Yes	Yes

VII. Conclusion

In this paper, Sun threshold proxy signature scheme has been analysis. The scheme is based on discrete logarithm assumption. The security of Sun is undeniable threshold proxy signature scheme with known signers. We find that in Sun scheme, a malicious original signer can forge a valid proxy signature on any message without the agreement of the proxy group. We also suggest an efficient scheme which involves the characteristics and gains of the RSA cryptosystem which is a popular security scheme.

Acknowledgment

The author wishes to extend his thanks to the University of Bedfordshire, computer science Department for their helpful suggestions and supports.

References

[1] Mambo M., Usuda K., and Okamoto E., "Proxy Signatures for Delegating Signing Operation", Proceeding of 3rd ACM Conference on Computer and Communications Security, ACM Press, pp. 48-57, 1996.

[2] Kim H., Baek J., Lee B., and. Kim K, "Secrets for Mobile Agent Using Onetime Proxy Signature", Cryptography and Information Security 2001, Volume 2/2, pp. 845-850, 2001.

[3] Lee B., Kim H., and Kim K., "Secure Mobile Agent Using Strong Non-designated Proxy Signature," Proceeding of ACISP 2001, pp. 474-486, 2001.

[4] Sun M., "Design of time-stamped proxy signatures with traceable receivers", IEE Proceedings: Computers and Digital Techniques, 2000, vol. 147, no. 6, pp. 462-466.

[5] Seo S., Shim K., and Lee S., "A mediated proxy signature scheme with fast revocation for electronic transactions", Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business, Aug 22-26, 2005, LNCS 3592, German: Springer, 2005, pp. 216-225, 2005.

[6] Shamir A., "How to Share a Secret", Communications of the ACM, Volume 22, No. 11, pp. 612-613, 1979.

[7] Zhang K, "Threshold Proxy Signature Schemes, "Information Security Workshop", Japan, pp. 191-197, 1997.

[8] Sun H., "An Efficient Nonrepudiable Threshold Proxy Signatures with Known Signers", Computer Communications 22(8), pp. 717-722, 1999.

[9] Hsu C., and T. Wu, "New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers", the Journal of Systems and Software 58(2001), pp. 119-124, 2001.

[10] Yang C., Tzeng S. and M. Hwang, "On the Efficiency of Nonrepudiable Threshold Proxy Signatures with Known Signers", Journal of Systems & Software 22(9), pp. 1-8, 2003.

[11] Tzeng S., Hwang M., and Yang C., "An Improvement of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers", Computers & Security 23, pp. 174-178, 2004.

[12] Yuan Yumin, "A Threshold Proxy Signature Scheme with Non-Repudiation and Anonymity", Computer and Information Sciences-Proceedings of ISCIS 2006, 21st International Symposium, Istambul, Turkey, November 1-3, 2006.

[13] Qi Xie, Jilin Wang and Xiuyuan Yu, "Improvement of Nonrepudable Threshold Multy-Proxy Threshold Multi-Signature Scheme with Shared Verification", Journal of Electronics (China), Volume 24, 2007

[14] Hu, J., Zhang, J., "Cryptanalysis & Improvement of a Threshold Proxy Signature Scheme", Computer Standards & Interfaces, 2009.

[15] Pedersen T., "A Threshold Cryptosystem without Trusted Party", Proceeding of Advance in Cryptology-EUROCRYPTO'91, LNCS 547, Springer-Verlag, pp. 522-526, 1991.

[16] Feldman P., "A Practical Scheme for Non–Interactive Veriable Secret Sharing", Proceeding of 28th FOCS, IEEE, pp. 427-437, 1987.

[17] Hwang M, Lin I, and Lu K, "A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers", International Journal of Informatica, Volume 0, Number 0, 1-0, pp.1-14, 2012.

AUTHORS PROFILE

Sattar J Aboud is currently, a Visiting Professor in the Department of Computer at University of Bedfordshire, UK. He received his education from United Kingdom. Dr. Aboud has served his profession in many universities and he awarded the Quality Assurance Certificate of Philadelphia University, Faculty of Information Technology in 2002. Also, he awarded the Medal of Iraqi Council of Representatives for his conducting the first international conference of Iraqi Experts in 2008. His research interests include the areas of both symmetric and asymmetric cryptography, area of verification and validation, performance evaluation and e-payment schemes.