International Journal of Computer Applications (0975 - 8887)
Volume 157 - No.10, January 2017

A Secure and an Efficient ID-based Multi-Proxy Multi-Signature Scheme from Bilinear Pairings

Pankaj Sarde
Department of Mathematics
Rungta Engineering College
Raipur(CG), India

Amitabh Banerjee
Department of Mathematics
Govt. S. N. College, Nagri
Dhamtari(CG), India

C. L. Dewangan
Department of Mathematics
Govt. College, Fingeshwar
Gariyaband(CG), India

ABSTRACT

Identity based(ID-based) public key cryptosystem gives an efficient alternative for key management as compared to certificate based public key setting. Proxy signature is a signature scheme that an original signer delegates his/her signing capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. Due to various application of the bilinear pairings in cryptography, many identity based signature scheme have been proposed. In this paper, we propose an identity based multi-proxy multi-signature scheme from bilinear pairings. The proposed scheme is more efficient than the multi proxy multi-signature scheme given by Li and Chen [2]. Moreover, The proposed scheme satisfies all the security requirements of a proxy signature given in [10]

Keywords

ID-based signature scheme, Bilinear pairing, Multi-proxy multi-signature

1. INTRODUCTION

In a certificate-based public key system, before using the public key of a user, the participants must verify the certificate of the user at first. As a consequence, this system requires a large storage and computing time to store and verify each users public key and the corresponding certificate. In 1984 Shamir [1] proposed ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting. Since then, many ID-based encryption and signature schemes [13, 14, 15, 3] have been proposed. The main idea of ID-based cryptosystems is that the identity information of each user works as his/her public key, in other words, the users public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA). ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. The bilinear pairings, namely the Weil-pairing and the Tate-pairing of algebraic curves, are important tools for research on algebraic geometry. They have been found various applications in cryptography recently [3, 4, 5, 6]. More precisely, they can be used to construct ID-based cryptographic schemes. The concept of proxy signature was introduced by Mambo, Usuda and Okamoto [7] in 1996. Their proxy signature scheme allows an original signer to delegate his signing right to a proxy signer to sign the message on behalf of an original signer. Later, the verifier, which knows the public keys of original signer and a proxy signer can check a validity of a proxy signature issued by a proxy signer. There are three different types of delegations: full delegation, partial delegation and delegation by warrant. In a full delegation proxy signature scheme, a proxy signer uses the same private key as an original signer and creates the proxy signature as an original signer does. The drawback of a full delegation comes from a difficulty of distinctive between an original signer and a proxy signer. In a partial delegation proxy signature scheme, the original signer derives the proxy key from his private key and passes it to the proxy signer in a secure channel. In the proxy signature scheme with delegation by warrant, an original signer provides the proxy signer a special message namely warrant. The warrant certifies that a proxy signer is legal and contains signer identity, delegation period and the types of a message on which a proxy signer can sign. According to the privilege of original signer, the proxy signatures can be categorized in proxy protected and proxy unprotected schemes. In unprotected proxy signature scheme, a proxy signature is generated by both the proxy signer and an original signer. In this case, the verifier cannot distinguish the identity of a signer. In the protected proxy signature scheme, a proxy signature is generated by the proxy signature key of an original signer and also with a private key of a proxy signer. the proxy signature can be categorized in multi-proxy signature, proxy multi-signature and multi-proxy multi-signature. The concept of multi-proxy signature is applicable when an original signer needs to delegate its signing right to a group of proxy signers. The idea of multi-proxy signature was introduced by Hwang and Shi [8]in 2000. Another kind of proxy signature schemes is multi-proxy multi-signature schemes proposed by Hwang [9]. In multi-proxy multi-signature schemes, an original group of signers can authorize a group of proxy signers under the agreement of all signers both in the original group and the proxy group. Then only the cooperation of all signers in proxy group can generate multi-proxy multi-signatures. multi-proxy multi-signatures can play important roles in the following scenario: For a large building, there are some conflict among the constructors and the householders. All householders of the large building want to authorize a lawyer group as their agents. So a group of lawyers are authorized to act on behalf of all householders. In 2005, Li and Chen [2] proposed the ID-based multi-proxy signature, proxy multi-signature and multi-

proxy multi-signature schemes from bilinear pairings. Their multi-proxy signature and proxy multi-signature schemes can be regarded as special cases of corresponding variants of ID-based threshold signature schemes. They have also proposed the multi-proxy multi-signature scheme, combining the multi-proxy signature and proxy multi-signature generating a certificate for the group of proxy signers.

In this paper, we propose a secure an efficient ID-based multi-proxy multi-signature scheme from bilinear pairings. The proposed scheme improved the efficiency of multi-proxy multi-signature scheme in [2].

The rest of this paper is organized as follows: In section 2, we introduce the bilinear pairing, some related mathematical problems and the security requirements of a proxy signature and a formal security model of ID-based proxy signature scheme. Briefly review the ID-based multi-proxy multi-signature scheme of Li and Chen is given in section 3. The proposed scheme is described in section 4. Analyze the security properties and performance analysis of proposed scheme are given in section 5. The concluding remarks are provided in section 6.

2. PRELIMINARIES

In this section, we introduce the bilinear pairing, some related mathematical problems and the security requirements of a proxy signature and a formal security model of ID-based proxy signature scheme.

2.1 Bilinear Pairing

Let G_1 be a cyclic additive group produced by P, with a prime order q, and G_2 be a cyclic multiplicative group with the same order q. Then, $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing with the following properties:

—**Bilinearity:** $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in Z_q$.

—**Non-degeneracy:** There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

—**Computability:** There exists an efficient algorithm to calculate $e(P, Q)$ for all $P, Q \in G_1$.

A bilinear map satisfied the three properties above is said to be an admissible bilinear map. It is well known that Weil and Tate pairings related with supersingular elliptic curves or abelian varieties can be modified to get such bilinear maps.

2.2 Some Mathematical Problems

—**DLP (Discrete Logarithm Problem:)** Given two group elements P and Q , find an integer $a \in Z_q^\star$ such that $Q = aP$ whenever such an integer exists.

—**DDHP (Decision Diffie-Hellman Problem:)** For $a, b, \in Z_q^\star$, given P, aP, bP, cP , decide whether $c \equiv ab \bmod q$. If it holds, (P, aP, bP, cP) is called a valid Diffie-Hellman tuple.

—**CDHP(Computational Diffie-Hellman Problem:)** For $a, b \in Z_q^\star$, given P, aP, bP, compute abP.

—**GDHP (Gap Diffie-Hellman Problem):** A class of problem where DDHP is easy while CDHP is hard. When the DDHP is easy but the CDHP is hard on the group G_1 , we call G_1 a gap Diffie-Hellman (GDH)group.

2.3 Security requirement for a proxy signature

A secure proxy signature scheme should satisfy the following security properties [10]

—**Strong unforgeability:** No one, other than the proxy signer, can generate a valid proxy signature.

—**Verifiability:** The signature can be verified by anyone, and the signed message should confirm to the delegation warrant. That means, any verifier can be convinced of the original signers agreement on the signed message.

—**Strong identifiability:** Identity of corresponding proxy signer can be determined by anyone.

—**Strong undeniability:** The proxy signer cannot deny his signature, he has made ever.

—**Prevention of misuse:** The proxy signer cannot sign any message, which has not been authorized by the original signer. Or alternatively, It should be confident that proxy key cannot be used for other purposes. In the case of misuse, the responsibility of proxy signer should be determined explicitly.

2.4 Security model of ID-Based Proxy Signature

Security model of Id-based proxy signature scheme [11] detailed given below:

—**ParamGen:** This algorithm outputs the systems public parameter param and systems master key s, taking the security parameter k as an input.

—**Key Extract:** This algorithm gives secret keys S_{ID_A}; S_{ID_B} of original signers A and proxy signers B, taking their identities ID_A and ID_B as inputs.

—**Standard Sign:** This algorithm outputs the standard signature σ_s, taking message m, systems parameter param and secret key S_{ID} as input.

—**Standard Verify:** Taking systems parameter param, standard signature σ_s, message m, the signers identity ID, this algorithm outputs True if σ_s is a valid signature, False otherwise.

—**Delegation Gen:** Inputs in this algorithm are systems parameter param, the original signers secret key S_{ID_A}, and the warrant to be signed. And output is delegation σ_w, which is generated using the standard signing algorithm.

—**ProxySign:**This algorithm takes systems parameter param, the warrant w, delegation σ_w, the secret key S_{ID_B} of proxy signer, the message m to be signed and outputs proxy signatureσ.

—**ProxyVerify:** This algorithm takes inputs the systems parameter param, original signers identity ID_A, proxy signers identity ID_B, the warrant w, the message m and the signature σ on message m and outputs True if the proxy signature σ is a valid signature on message m, False otherwise.

3. BRIEFLY REVIEW OF ID-BASED MULTI-PROXY MULTI-SIGNATURE SCHEME OF LI AND CHEN

In this section, we briefly review the ID-based multi-proxy multi-signature scheme of Li and Chen [2]with the same notations as in [12]. For security analysis and other details one can refer [2]

—**System setup:** For a given security parameter k, let G_1 and G_2 be two groups of prime order q, and P be the generator of G_1. Define a bilinear map $e : G_1 \times G_1 \rightarrow G_2$. The PKG selects master key $s \in_R Z_q^\star$, computes public key $P_{pub} = sP$ and

keeps the master key s secret. Define cryptographic hash functions $H_1 : \{0,1\}^\star \to Z_q$, $H_2 : \{0,1\}^\star \to G_1$. Systems public parameter is $param = \{G_1, G_2, k, e, q, P, P_{pub}, H_1, H_2\}$.

—**Extraction:** For $1 \le i \le n$, $Q_{ID_{A_i}}$ and $d_{ID_{A_i}} = sH_2(ID_{A_i})$ are public and private keys respectively, for the n original signers A_i, with identity $\{ID_{A_i}\}$. Similarly, for $1 \le j \le l$, $Q_{ID_{B_j}} = H_2(ID_{B_j})$ and $d_{ID_{B_j}} = sH_2(ID_{B_j})$ are public and private keys respectively, for the l proxy signers B_j, with identity $\{ID_{B_j}\}$.

—**Proxy certificate generation:** In this phase, all proxy signers cooperate with all of the original signers to generate the certificate. Here m_w is the message warrant. In successfully completion of this phase, each proxy signer B_j , for $1 \le j \le l$, gets a proxy certificate (U, V).
- For $1 \le i \le n$, each A_i
chooses $x_{a_i} \in_R Z_q^\star$
computes $U_{a_i} = x_{a_i} P$
broadcasts U_{a_i} to the other $(n-1)$ original signers l proxy signers.
- For $1 \le j \le l$, each B_j
chooses $x_{b_j} \in_R Z_q^\star$
computes $U_{b_j} = x_{b_j} P$
broadcasts U_{b_j} to the other $(l-1)$ proxy signers n original signers.
- All of the Signers A_i and B_j,
compute $U = \sum_{i=1}^{n} U_{a_i} + \sum_{j=1}^{l} U_{b_j}$
- For $1 \le i \le n$, each A_i, computes
$V_{a_i} = H_1(m_w \parallel U) d_{ID_{A_i}} + x_{a_i} P_{pub}$
broadcast V_{a_i} to the chirman of original group.
- For $1 \le j \le l$, each B_j, computes
$V_{b_j} = H_1(m_w \parallel U) d_{ID_{B_j}} + x_{b_j} P_{pub}$
broadcast V_{b_j} to the chirman of original group.
- The chairman confirms V_{a_i} and V_{b_j} by checking

$$e(P, V_{a_i}) = e(U_{a_i}, P_{pub}) e(P_{pub}, Q_{ID_{A_i}})^{H_1(m_w \| U)}$$

, $1 \le i \le n$

$$e(P, V_{b_j}) = e(U_{b_j}, P_{pub}) e(P_{pub}, Q_{ID_{B_j}})^{H_1(m_w \| U)}$$

, $1 \le j \le l$ respectively. If all of the above equalities hold, the chairman computes

$$V = \sum_{i=1}^{n} V_{a_i} + \sum_{j=1}^{l} V_{b_j}$$

and broadcasts V to the all original and proxy signers. Finally, members of the proxy group are authorized to act as proxy agents for the group of n original signers with certificate (U, V)

—**Multi-proxy multi-signature generation:** If the l proxy signers want to sign a message m on behalf of the n original signers, they perform the following steps. One proxy signer in the proxy group, plays the role of clerk to combine all partial proxy signatures to generate the final multi-proxy multi-signature on message m with warrant m_w.
- For $1 \le j \le l$, each proxy signer B_j
Chooses $t_j \in_R Z_q^\star$
computes $R_j = t_j P$
broadcasts his R_j to the other $(l-1)$ proxy signers.
- For$1 \le j \le l$,each proxy signer B_j
computes $R = \sum_{j=1}^{l} R_j$ and
$S_j = H_1(m \parallel) d_{ID_{b_j}} + t_j V$ sends (R_j, S_j) to the clerk as his partial proxy signature on m
- For $1 \le j \le l$, the clerk verifies the partial proxy signature by checking the equation

$$e(P, S_j) = e(R_j, V) e(P_{pub}, Q_{ID_{B_j}})^{H_1(m \| R)}$$

If the above equality holds for $1 \le j \le l$, the final multi-proxy multi-signature on the message m is generated as $(m_w, (R, S), (U, V))$ by the clerk where $S = \sum_{j=1}^{l} S_j$

—**Verification:** Receiving the multi-proxy multi-signature $(m_w, (R, S), (U, V))$, and the message m,the verifier proceeds as follows:
- Checks whether or not the message m conforms to the warrant m_w. If not, stop. Continue, otherwise.
- Checks whether or not the l proxy signers are authorized by the n original signers in the warrant m_w. If not, stop. Continue, otherwise.
- Verifies the warrant and the certificate (U, V) by the equation:

$$e(P, V) = e(U, P_{pub}) e(P_{pub} \sum_{i=1}^{n} Q_{ID_{A_i}} + \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_1(m_w \| U)}$$

- Accepts the multi-proxy multi-signature if and only if the following equality holds:

$$e(P, S) = e(R, V) e(P_{pub}, \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_1(m \| R)}$$

4. PROPOSED SCHEME

The proposed scheme divided into six phases: System setup phase, Extraction phase, Proxy certificate generation phase, Multi-proxy multi-signature generation phase, Verification phase.

—**System Setup Phase:** let G_1 and G_2 be two cyclic group of prime order q, and P be the generator of G_1. Define a bilinear map $e : G_1 \times G_1 \to G_2$. The PKG randomly selects a master key $s \in_R Z_q^\star$ and computes public key $P_{pub} = sP$. Define cryptographic hash function $H_1 : \{0,1\}^\star \to G_1, H_2 : \{0,1\}^\star \times G_1 \to Z_q^\star, H_3 : \{0,1\}^\star \times G_1 \to G_1, H_4 : \{0,1\}^\star \times G_1 \times G_1 \to G_1$. The PKG publishes system public parameters **params** $= \{G_1, G_2, k, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$

—**Extract:** Let for $1 \le i \le n$, A_i be the original signers with identity ID_{A_i}, for $1 \le j \le l$, B_j be the proxy signers with identity ID_{B_j}. The PKG computes public and private keys of A_i as $Q_{ID_{A_i}} = H_1(ID_{A_i})$ and $S_{ID_{A_i}} = sQ_{ID_{A_i}}$ respectively. Similarly the public and private keys of B_j as $Q_{ID_{B_j}} = H_1(ID_{B_j})$ and $S_{ID_{B_j}} = sQ_{ID_{B_j}}$

—**Proxy Certificate generation Phase:** In this phase, all of the original signers A_i , for $1 \le i \le n$ co-operate with all of proxy signers B_j, $for 1 \le j \le l$ to generate the proxy certificate. For this, we use the warrant m_w, which specifies what kind of message is delegated, delegation period, identity information of original signers and proxy signers.
- For $1 \le i \le n$, each original signers A_i
selects $x_{a_i} \in_R Z_q^\star$ and
computes $U_{a_i} = x_{a_i} P$
and broadcasts U_{a_i} to $(n-1)$ original signers and l proxy signers.

- For $1 \leq j \leq l$, each proxy signers B_j
selects $x_{b_j} \in_R Z_q^\star$ and
computes $U_{b_j} = x_{b_j} P$
and broadcasts U_{b_j} to $(l-1)$ proxy signers and n original signers.
- All of the original signers A_i and proxy signers B_j computes

$$U = \sum_{i=1}^{n} U_{a_i} + \sum_{j=1}^{l} U_{b_j}$$

- For $1 \leq i \leq n$, original signers A_i computes

$$V_{a_i} = H_2(ID_{A_i} \parallel U) S_{ID_{A_i}} + x_{a_i} H_3(m_w \parallel U)$$

each A_i sends their V_{a_i} to a chairman of the original group
- For $1 \leq j \leq l$, original signers B_j computes

$$V_{b_j} = H_2(ID_{B_j} \parallel U) S_{ID_{B_j}} + x_{b_j} H_3(m_w \parallel U)$$

each B_j sends their V_{b_j} to a chairman of the original group.
- The chairman receiving V_{a_i} from each A_i, confirms the validity of V_{a_i} for $i = 1, 2, 3, ..., n$ such that

$$e(P, V_{a_i}) = e(P_{pub}, Q_{ID_{A_i}})^{H_2(ID_{A_i}, U)} e(U_{a_i}, H_3(m_w \parallel U))$$

- Similarly, the chairman also confirms the validity of V_{b_j} for $j = 1, 2, 3, ..., l$ such that

$$e(P, V_{b_j}) = e(P_{pub}, Q_{ID_{B_j}})^{H_2(ID_{B_j}, U)} e(U_{b_i}, H_3(m_w \parallel U))$$

- If all V_{a_i} and V_{b_j} holds, then chairman combine them as

$$V = \sum_{i=1}^{n} V_{a_i} + \sum_{j=1}^{l} V_{b_j}$$

and broadcasts V to the n original signers and l proxy signers.
- After receiving (U, m_w, V), each proxy signers confirms its validity by checking

$$e(P, V) = e(P_{pub}, \sum_{i=1}^{n} Q_{ID_{A_i}})^{H_2(ID_{A_i} \parallel U)} e(P_{pub}, \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_2(ID_{B_j} \parallel U)} e(U, H_3(m_w \parallel U)) \quad (1)$$

If it is true, then each proxy signers accept the proxy certificate (U, V) on the message warrant m_w, otherwise request for a new one.

—**Multi-proxy multi-signature generation phase:** Suppose that l proxy signers want to sign a message m on behalf of original signers A_i. For this, proxy signers B_j do the following steps such that
- First each proxy signers B_j for $1 \leq j \leq l$ generate proxy secret key

$$S_{p_j} = V + H_4(m_w \parallel U \parallel V) S_{ID_j}$$

- Now each proxy signers B_j $(1 \leq j \leq l)$ randomly select an integer $t_j \in_R Z_q^\star$ and computes $R_j = t_j P$, broadcasts to the other $(l-1)$ proxy signers
- Each proxy signers B_j $(1 \leq j \leq l)$ computes

$$R = \sum_{j=1}^{l} R_j$$

and

$$S_j = S_{p_j} H_2(ID_{B_j} \parallel R) + t_j H_3(m \parallel R)$$

sends (R, S_j) to the clerk as his partial proxy signature on the message m.
- After receiving (R, S_j) from proxy signers, the Clerk verifies the partial proxy signatures on the message m such that

$$e(P, S_j) = e(R_j, H_3(m \parallel R)) e(P, V)^{H_2(ID_{B_j} \parallel R)} e(P_{pub}, Q_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V) H_2(ID_{B_j} \parallel R)}$$

If all the partial proxy signature are correct, Clerk combine them as $S = \sum_{j=1}^{l} S_j$. Thus multi-proxy multi-signature on the message m is $(m_w, m, (U, V), (R, S))$

—**Verification Phase:** After receiving the multi-proxy multi signature $(m_w, m, (U, V), (R, S))$, the verifier check the following steps
- Checks whether or not the message m confirms to the warrant m_w. If not, stop. Continue otherwise.
- Check whether or not the l proxy signers are authorized by the group of n original signers in the warrant m_w. If not, stop. Continue otherwise.
- Validity of multi-proxy multi-signature if the following equation hold

$$e(P, S) = e(R, H_3(m \parallel R)) e(P, V)^{H_2(ID_{B_j} \parallel R)} e(P_{pub}, \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V) H_2(ID_{B_j} \parallel R)} \quad (2)$$

5. ANALYSIS OF PROPOSED SCHEME

In this section, we prove the correctness of verification. The proposed scheme also satisfies all the security requirement of proxy signature which is described in [10]. We will make discussion on the performance of [2] and proposed scheme.

5.1 Correctness

To prove (1)
$e(P_{pub}, \sum_{i=1}^{n} Q_{ID_{A_i}})^{H_2(ID_{A_i} \parallel U)}$
$e(P_{pub}, \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_2(ID_{B_j} \parallel U)} e(U, H_3(m_w \parallel U)) =$
$(P, \sum_{i=1}^{n} S_{ID_{A_i}})^{H_2(ID_{A_i} \parallel U)} e(P, \sum_{j=1}^{l} S_{ID_{B_j}})^{H_2(ID_{B_j} \parallel U)}$
$e(\sum_{i=1}^{n} U_{a_i} + \sum_{j=1}^{l} U_{b_j}, H_3(m_w \parallel U)) =$
$e(P, \sum_{i=1}^{n} S_{ID_{A_i}} H_2(ID_{A_i} \parallel$
$U) + \sum_{j=1}^{l} S_{ID_{B_j}} H_2(ID_{B_j} \parallel U))$
$e(P, H_3(m_w \parallel U)(\sum_{i=1}^{n} x_{a_i} + \sum_{j=1}^{l} x_{b_j})) =$
$e(P, \sum_{i=1}^{n} (H_2(ID_{A_i} \parallel U) S_{ID_{A_i}}) + \sum_{j=1}^{l} (H_2(ID_{B_j} \parallel U) S_{ID_{B_j}})) e(P, H_3(m_w \parallel U)(\sum_{i=1}^{n} x_{a_i} + \sum_{j=1}^{l} x_{b_j}))$
$= e(P, \sum_{i=1}^{n} (H_2(ID_{A_i} \parallel U) S_{ID_{A_i}} + H_3(m_w \parallel U) x_{a_i})$
$+ \sum_{j=1}^{l} (H_2(ID_{B_j} \parallel U) S_{ID_{B_j}} + H_3(m_w \parallel U) x_{b_j})$
$e(P, \sum_{i=1}^{n} V_{a_i} + \sum_{j=1}^{l} V_{b_j}) = e(P, V)$

To prove (2)
$e(R, H_3(m \parallel R))e(P,V)^{H_2(ID_{B_j} \parallel R)}$
$e(P_{pub}, \sum_{j=1}^{l} Q_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V)H_2(ID_{B_j} \parallel R)}$
$= e(\sum R_j, H_3(m \parallel R))e(P,V)^{H_2(ID_{B_j} \parallel R)}$
$e(P, \sum_{j=1}^{l} S_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V)H_2(ID_{B_j} \parallel R)}$
$= e(P, \sum t_j H_3(m \parallel R))e(P,V)^{H_2(ID_{B_j} \parallel R)}$
$e(P, \sum_{j=1}^{l} S_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V)H_2(ID_{B_j} \parallel R)}$
$= e(P, \sum_{j=1}^{l} t_j H_3(m \parallel R) + VH_2(ID_{B_j} \parallel R))$
$e(P, H_4(m_w \parallel U \parallel V)H_2(ID_{B_j} \parallel R) \sum_{j=1}^{l} S_{ID_{B_j}})$
$= e(P, \sum_{j=1}^{l}(t_j H_3(m \parallel R) + \sum_{j=1}^{l}(H_4(m_w \parallel U \parallel V)S_{ID_{B_j}} +$
$V)H_2(ID_{B_j} \parallel R)))$
$= e(P, \sum_{j=1}^{l} t_j H_3(m \parallel R) + \sum_{j=1}^{l} S_{P_j} H_2(ID_{B_j} \parallel R))$
$= e(P, \sum_{j=1}^{l}(t_j H_3(m \parallel R) + S_{P_j} H_2(ID_{B_j} \parallel R)))$
$= e(P, \sum_{j=1}^{l} S_j)$
$= e(P, S)$

5.2 Security Analysis

In this section, we show that proposed scheme satisfies all the security requirement which is mentioned in 2.3

—**Strong Unforgeability:** There are four type of attacker in multi-proxy multi-signature scheme. first, third party who do not participate the issue of multi-proxy multi-signature scheme, second proxy signer who play an active part in signature process. Third original signer and fourth, signature owner. In multi-proxy multi-signature we use proxy signer and original signer secret key S_{ID_j} for $j = 1, 2, 3.....,l$ and S_{ID_i} for $i = 1, 2, 3, ...n$ respectively. without knowing the secret key, proxy signer, original signer, signature owner and third party can not generate a valid multi-proxy multi-signature. Since it is based on CDHP and CDHP in G_1 is hard.

—**Strong identifiability:** By warrant and proxy secret key, any one can determine the identity of proxy signers.

—**Verifiability:** Any verifier can verify the multi-proxy multi-signature scheme. Thus our scheme provide the public verifiability.

—**Strong Undeniability** In proposed multi-proxy multi-signature scheme, Clerk individual verify the validity of proxy signer's partial signature on the message m such that

$$e(P, S_j) = e(R_j, H_3(m \parallel R))e(P,V)^{H_2(ID_{B_j} \parallel R)} \\ e(P_{pub}, Q_{ID_{B_j}})^{H_4(m_w \parallel U \parallel V)H_2(ID_{B_j} \parallel R)}$$

, secret key S_{P_j} of proxy signers B_j and at the same time warrant m_w also contains the identity information of B_j involve in the verification process. Thus, no proxy signers can deny of his signature.

—**Prevention of misuse:** In proposed scheme, we use warrant m_w which contains delegation period, nature of message, identities of original signers and proxy signers etc. Due to using the warrant m_w, the proxy signers can sign messages that have been authorized by the original signer.

5.3 Efficiency Comparisons

We compare proposed scheme with that of multi-proxy multi-signature scheme which is described in [2].

Table 1. Verification Phase

Scheme	Pairing	Exponentiation	Hashing
Li Chen Scheme	6	2	2
Our Scheme	4	2	3

Thus proposed scheme is computationally and economically more efficient than in [2].

6. CONCLUSION

In this paper, we have proposed a secure and an efficient ID-based multi-proxy multi-signature scheme from bilinear pairings. In this paper, we have compared verification phase of Li and Chen scheme with proposed scheme. In this paper, we have also analyzed security property of proposed scheme. Proposed scheme is strongly satisfied the security properties of proxy signature schemes. We prove that proposed scheme is secure, efficient and correct.

7. REFERENCES

[1] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto 1984, LNCS 196, 47-53, Springer-Verlag, 1984.

[2] X. Li and K. Chen, ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings, Applied Mathematics and Computation, 169, 2005, pp. 437-450.

[3] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, 213-229, Springer-Verlag, 2001.

[4] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, 514-532, Springer-Verlag, 2001.

[5] A. Joux, The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems, ANTS 2002, LNCS 2369, 20-32, Springer-Verlag, 2002.

[6] D.Boneh and X.Boyen, Short Signatures Without Random Oracles. Eurocrypt 2004, LNCS 3027, 56-73, Springer-Verlag, 2004.

[7] M. Mambo, K. Usuda and E. Okmamoto, Proxy signatures:delegation of the power to sign message, IEICE Transaction Functional E79-A (9), 1996, pp.1338 - 1354.

[8] S. Hwang and C. Shi, A simple multi-proxy signature scheme, Proceedings of the 10th national conference on information security, Hualien, Taiwan, ROC; 2000, pp. 134-138.

[9] S. Hwang, C. Chen, New multi-proxy multi-signature schemes, Appl. Math. Comput. 147 (2004) 5767.

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

[11] W. Wu, Y. Mu, W. Susilo, J. Seberry and X. Huang, Identity-based proxy signature from pairing: In ATC 2007, LNCS 4610, Springer 2007, pp.22-31.

[12] F. Hesss, Efficient identity based signature scheme based on pairings, SAC'2002, Springer-Verlag, LNCS 2595, pp. 310-324.

[13] U. Maurer and Y. Yacobi, "Non-interactive public-key cryptography", proc. Eurocrypt '91, pp. 498-507.

[14] S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem", IEEE Journal on Selected Areas in Communication, vol. 7, no. 4, pp. 467-473, 1989.

[15] H. Tanaka, ”A realization scheme for the identity-based cryptosystem”, Proc. Crypto ’87, pp. 341-349, 1987.