ID-Based Directed Multi-Proxy Signature Scheme from Bilinear Pairings

B.Umaprasada Rao buprasad@yahoo.co.in
Research scholar
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam. A.P, INDIA.

Dr.P.Vasudeva Reddy vasucrypto@yahoo.com
Associate Professor
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam, A.P, INDIA.

Abstract

In a multi-proxy signature scheme, an original signer delegates his signing power to a group of proxy signers. Then the group of proxy signers cooperatively generates a multi-proxy signature on behalf of the original signer; and any one can verify the validity of the multi-proxy signature. But, when the signed message is sensitive to the signature receiver, it is necessary to combine the concepts of multi-proxy signatures with directed signatures. In this paper, we propose an identity based directed multi-proxy signature scheme using bilinear pairings. This scheme allows a group of proxy signers to generate a valid multi-proxy signature to a designated verifier. The designated verifier can only directly verify the multi-proxy signature generated by a group of proxy signers issued to him on behalf of the original signer and, in case of trouble or if necessary, he can convince any third party about the validity of the signatures. Finally, we discuss the correctness and security analysis of the proposed scheme.

Keywords: Public Key Cryptography, Proxy Signature Scheme, Multisignature Scheme, Proxy Signature Scheme, Bilinear Pairing, CDH Problem.

1. INTRODUCTION

Proxy signature, as an important cryptographic primitive, was firstly introduced by Mambo, Usuda, and Okamoto in 1996 [1]. In a proxy signature scheme, an original signer is allowed to delegate his signing power to a designated person called the proxy signer and the proxy signer is able to sign the message on behalf of the original signer. There are three types of delegation: full delegation; partial delegation and delegation by warrant. In full delegation, the original signer gives its private key to the proxy signer. In partial delegation, the original signer produces a proxy signature key from its private key and gives it to the proxy signer. The proxy signer uses the proxy signature key to sign. As far as delegation by warrant is concerned, warrant is a certificate composed of a message part and a public signature key. The proxy signer gets the warrant from the original signer and uses the corresponding private key to sign.

Since the proxy signature concept was proposed, various kinds of proxy signature schemes have been proposed such as threshold proxy signatures [2, 3, 4, 5, 6], multi proxy signatures [7, 8, 9], proxy multisignatures [10, 9, 8], proxy blind signatures [11, 12], multi proxy multi signatures [13, 14], ordered multi proxy [15], multi proxy multi signcryption [16,17] etc. In threshold proxy signature schemes, a group of *n* proxy signers share the secret proxy signature key. To produce a valid proxy signature on the message *m,* individual proxy signers produce their partial signatures on that message, and combine them into a full proxy signature on *m.* In a *(t, n)* threshold proxy signature scheme, the original signer authorizes a proxy group with *n* proxy members. Only the cooperation of *t* or more proxy members is allowed to generate the proxy signature. Threshold signatures are motivated both by the demand which arises in some organizations to have a group of employees agree on a given message or document before signing, and by the need to protect signature keys from attacks of internal and external adversaries.

In 1999, Sun proposed a threshold proxy signature scheme with known signers [4]. Then Hwang et al. [3] pointed out that Sun's scheme was insecure against collusion attack. By the collusion, any *t* - 1 proxy signers among *t* proxy signers can cooperatively obtain the secret key of the remainder one. They also proposed an improved scheme which can guard against the collusion attack. After that, [2] showed that Sun's scheme was also insecure against the conspiracy attack. In the conspiracy attack, *t* malicious proxy signers can impersonate some other proxy signers to generate valid proxy signatures. To resist the attack, they also proposed a scheme. Hwang et al pointed out [18] that the scheme in [3] was also insecure against the attack by the cooperation of one malicious proxy signer and the original signer.

As a special case of the threshold proxy signature, the multi-proxy signature scheme was first introduced by Hwang and Shi [7]. In a multi-proxy signature scheme, an original signer could authorize a group of proxy members and only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. Multi proxy signature scheme can be regarded as a special case of the (t,n) threshold proxy signature scheme [5] for$t=n$. It plays an important role in the following scenario: Suppose a president of a company needs to go on a business trip, during the trip he will receive many important documents must be signed by him. Some may need to be responded to quickly. To solve this problem, before going on a trip, the president can delegate his signing power to every department manager of the company. Then the document must be signed jointly by these department managers authorized by the president of the company. One solution to the case of this problem is to use a multi-proxy signature scheme.

A contrary concept, called proxy-multisignature is introduced by Yi et al. in 2000 [10], where a designated proxy signer can generate the signature on behalf of a group of original signers. Hwang and Chen [13] introduced the multi-proxy multi-signature scheme. Only the cooperation of all members in the original group can authorize a proxy group; only the cooperation of all members in the proxy group can sign messages on behalf of the original group.

Some designated verifier multi proxy signatures are also proposed in the literature [19]. In these schemes, an original signer could authorize a group of proxy members and only the cooperation of all the signers in the proxy group can generate the proxy signatures to a designated verifier on behalf of the original signer. The designated verifier only can directly verify the multi-proxy signature issued to him. In these schemes, the designated verifier cannot convince any third party about the validity of the multi-proxy signatures. To solve this problem, it necessary to combine the concepts of multi-proxy signatures with the directed signatures [20, 21, 22, 23].

Plenty of multi-proxy signature schemes have been proposed under the CA-based public key systems. The concept of ID-based public key system, proposed by Shamir in 1984 [24], allows a user to use his identity as the public key. It can simplify key management procedure compared to CA-based system, so it can be an alternative for CA-based public key system in some occasions, especially when efficient key management and moderate security are required. Many ID-based schemes have been proposed after the initial work of Shamir, but most of them are impractical for low efficiency. Recently, the bilinear pairings have been found various applications in cryptography, more precisely; they can be used to construct ID-based cryptographic schemes [25, 26, 27, 28, 29].

Motivated by the mentioned above, in this paper, based on Hess ID-based signature scheme [28], a directed multi-proxy signature scheme is proposed. In the proposed scheme, the designated verifier can only directly verify the multi-proxy signature generated by a group of proxy signers issued to him, on behalf of the original signer, and he can convince any third party about the validity of the signatures. To the best of our knowledge there is no existing scheme on this concept. The proposed scheme can provide the security properties of proxy protection, verifiability, strong identifiability, strong unforgeability, strong nonrepudiability, distinguishability, and prevention of misuse of proxy signing power.

The rest of the paper is organized as follows. Section 2 briefly explains the bilinear pairings and some computational problems on which of our scheme is based. The syntax and security model of ID-based Directed Multi Proxy Signature Scheme is given in Section 3. We then present our ID-based Directed Multi Proxy Signature (ID-DMPS) Scheme in Section 4. The correctness and security analysis of the proposed scheme is given in Section 5. Section 6 concludes this paper.

2. PRELIMINARIES

In this section, we will briefly review the basic concepts on bilinear pairings and some related mathematical problems.

2.1 Bilinear Pairings

Bilinear pairing is an important cryptographic primitive and has been widely adopted in many positive applications in cryptography.

Let G_1 be a additive cyclic group generated by P, whose order is a prime q, and G_2 be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P,Q)^{ab}$, for all $P,Q \in G_1$ and all $a,b \in Z_q^*$.
2. Non –degenerate: There exists $P,Q \in G_1$ such that $e(P,Q) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

Such a pairing may be obtained by suitable modification in the Weil-pairing or the Tate-pairing on an elliptic curve defined over a finite field [25].

2.2 Computational Problems

Now, we give some computational problems, which will form the basis of security for our scheme.

Decisional Diffie-Hellman Problem (DDHP): For $a,b,c \in_R Z_q^*$, given $P,\ aP, bP, cP$ in G_1 , decide whether $c \equiv ab \bmod q$.

Computational Diffie-Hellman Problem (CDHP): For $a,b,c \in_R Z_q^*$, given $P,\ aP,\ bP$ in G_1 Compute abP.

Bilinear Diffie-Hellman Problem (BDHP): For $a,b,c \in_R Z_q^*$, given $P,\ aP,\ bP, cP$ in G_1 , compute $e(P,P)^{abc}$ in G_2.

Gap Diffie-Hellman Problem: A class of problems, where DDHP can be solved in polynomial time but no probabilistic algorithm exists that can solve CDHP in polynomial time.

Such groups can be found in supersingular elliptic curve or hyperelliptic curve over finite fields, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [25].

3. SYNTAX AND SECURITY REQUIREMENTS FOR ID-DMPS SCHEME

In this section, we give formal model and some security requirements for our ID-based directed multi-proxy signature scheme (ID-DMPS).

3.1 Syntax of ID-Based Directed Multi-Proxy Signature Scheme

Our scheme has five phases described as follows:
In our identity-based multi-proxy signature scheme, there is an original signer and a group of proxy signers. Let **O** be the original signer and $L=\{PS_1,PS_2,.....,PS_n\}$ be the group of proxy signers designated by **O**. Sometimes there may be a clerk or a chairman of the group. For $i\in\{1,2,..,n\}$, PS_i has an identity IDs_i, **O** has an identity ID_o.

Our ID-DMPS scheme consists of the following five algorithms.

- **Setup:** This algorithm is run by the PKG on input a security parameter $l\in N$, and generates the public parameters of the scheme and a master secret $<s>$. The PKG publishes system parameters as *params* and keeps the $<s>$ as secret.

- **Extract:** Given an identity ID, *params*, this algorithm generates the private key d_{ID} of ID. The PKG will use this algorithm to generate private keys for all participants in the scheme and distribute the private keys to their respective owners through a secure channel.

- **Generation of the Proxy Key:** This is a protocol between the original signer and all proxy signers. All participants input their identities $ID_{s_i}, 0\leq i\leq n,$ the proxy signers also take as input their private keys $d_{ID_{s_i}}, 1\leq i\leq n,$ and the delegation warrant ω which includes the type of the information delegated, the period of delegation etc. The original signer also inputs his secret key d_{IDo}. As a result of the interaction, every proxy signer outputs a *partial proxy signing key* $SKP_i(1\leq i\leq n).$

- **Multi-proxy Signature Generation:** This is a randomized algorithm. Every PS_i takes input his partial signing key $SKP_i(1\leq i\leq n),$ the warrant m_ω,the designated verifier's identity ID_V , and the message $M\in\{0,1\}^*$. In the end, outputs a *directed multi-proxy signature* σ on the message M on behalf of the original signer.

- **Multi-proxy Direct Verification:** It is a deterministic algorithm. It takes input the identities $ID_{s_i}, 0\leq i\leq n,$ the warrant ω, the message M and a directed multi-proxy signature σ for M, the algorithm outputs 1 if σ is a valid multi-proxy signature for M by the proxy signers on behalf of the original signer, and outputs 0 otherwise.

- **Multi-proxy Public Verification:** It is a deterministic algorithm. It takes identity of the original signer ID_o, identities of the proxy signers IDs_i, identity of the designated verifier ID_V, message M, warrant ω, Aid provide by ID_V or Clark and multi-proxy signature σ as input, outputs 1if σ is valid or 0 otherwise.

3.2 Security Requirements of ID-Based Directed Multi Proxy Signature

The following are general security requirements of the proposed scheme.

- **Verifiability:** From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.
- **Strong Identifiably:** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
- **Strong Undeniability:** Once a proxy signer creates a valid proxy signature of an original signer, he cannot repudiate the signature creation.
- **Distinguishability:** Proxy signatures are distinguishable from normal signatures by everyone.
- **Prevention of Misuse**: The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature. That is, he cannot sign, with the proxy key, messages that have not been authorized by the original signer.
- **Strong Unforgeability:** A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.
- **Strong Designated Verifiability:** The designated verifier uses his/her secret key to verify the proxy signature generated by a proxy signer on behalf of the original signer to designated verifier. So, only the designated verifier can verify the proxy signature issued to him.

4. PROPOSED SCHEME ID-BASED DIRECTED MULTI-PROXY SIGNATURE SCHEME FROM BILINEAR PAIRINGS

The proposed scheme involves four roles: the private key generator (PKG), the original signer, a set of proxy signers $L=\{PS_1,PS_2,.....,PS_n\}$ and the verifier. It consists of the following Six algorithms.

Setup: Given security parameter l, the PKG chooses groups G_1 and G_2 be additive and multiplicative groups of prime order $q>2^l$ with a bilinear pairing $e:G_1 \times G_1 \to G_2$ and a generator P of G_1. PKG then selects $s\in Z_q^*$ randomly and compute the public key $P_{pub}=sP$, also picks cryptographic hash functions $H_1,H_2:\{0,1\}^* \to G_1^*$ and $h:\{0,1\}^* \times G_2 \to Z_q^*$. The private key generator PKG now publishes system parameters as $params =< G_1,G_2,q,e,P,P_{pub},H_1,H_2,h>$, and keeps $<s>$ secret as the master secret key.

Private key Extraction: Let the original signer identity ID_o and his private key $d_{ID_o}=sQ_{ID_o}=sH_1(ID_o)$, and $\{PS_i\}$ be the proxy signers with identity $\{IDs_i\}$ and their corresponding private key $d_{IDs_i}=sQ_{IDs_i}=sH_1(IDs_i)$, for $1\le i\le n$.

Generation of the Proxy Key: To delegate the signing power to proxy signers, the original signer uses Hess's ID-based signature scheme [28] to generate the signed warrant m_w and each proxy signer PS_i computes his proxy key SKP_i.

- The original signer computes $U_o = e(P,P)^{K_o}$, where $k \in_R Z_q^*$, $H_o = H_2(ID_o, m_w, U_o)$, $V_o = h(U_o, H_o)$ and then computes $W_o = V_o d_{ID_o} + k_o P$.
- The signature on m_w is the warrant $\langle m_w, W_o, V_o \rangle$ then he sends $\langle m_w, W_o, V_o \rangle$ to each proxy signer in the proxy group L.
- Each $PS_i \in L$ verifies the validity of the signature on m_w by computing $U_o = e(W_o, P)\, e(Q_{ID_o}, P_{pub})^{-V_O}$ and $H_o = H_2(ID_o, m_w, U_o)$. Accepts the signature if and only if $V_o = h(U_o, H_o)$.

If the signature valid, each PS_i computes the *proxy key* SKP_i as $SKP_i = V_o d_{IDs_i} + W_o$.

Multi-Proxy Signature Generation: Suppose the proxy group L want to sign a delegated message m, on behalf of the original signer, to the designated verifier V. Each proxy signer PS_i generates the partial signature and an appointed clerk C, who is one of the proxy signers, combines the partial proxy signatures to generate the final multi-proxy signature.

- Each PS_i randomly selects two integers $k_i, r_i \in_R Z_q^*$, computes $U_{P_i} = e(P,P)^{k_i}$, $R_{P_i} = r_i Q_{IDs_i}$, $L_{P_i} = e\left(d_{IDs_i}, r_i Q_{IDv}\right)$ and broadcast U_{P_i}, L_{P_i} to the remaining (n-1) signers.
- Each PS_i computes $U_P = \prod_{i=1}^{n} U_{P_i}$, $L_P = \prod_{i=1}^{n} L_{P_i}$, $R_P = \sum_{i=1}^{n} R_{P_i}$, $V_P = h(U_P, H_P)$ and broadcast to the clerk .
- Each proxy signer also computes $V_{P_i} = h(U_{P_i}, H_P)$ and $W_{P_i} = V_P SKP_i + k_i P,$ where $H_P = H_2(M, L_P)$.

Finally the individual proxy signature of message m is $\langle V_{P_i}, W_{P_i}, R_{P_i} \rangle$.

- All the proxy signers send their partial signatures to the clerk C. The clerk verifies each individual signature by checking the equality

$$V_{P_i} = h\left(H_2(M, L_P), e(W_{P_i}, P)\left(e\left(Q_{ID_o} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o \right)^{-V_P} \right).$$

Once all individual proxy signatures are correct, the clerk C computes $W_P = \sum_{i=1}^{n} W_{P_i}$.

The valid directed multi-proxy signature is the tuple $\sigma = \langle m, m_w, V_P, W_P, R_p, U_o \rangle$.

Direct Verification: The designated verifier ID_V first evaluate

$$U_P = e(W_P, P)\left(e\left(\sum_{i=1}^{n}\left(Q_{ID_o} + Q_{IDs_i}\right), P_{pub} \right)^{V_O} .U_o^n \right)^{-V_P}$$ and $H_P = H_2\left(m, e\left(d_{ID_V}, R_P\right)\right)$. He then accepts the signature if and only if $V_P = h(H_P, U_P)$.

Public Verification: In case of trouble or if necessary, any third party T can verify the validity of multi-proxy signature with the help of the $Aid = e\left(d_{ID_V}, R_P\right) = L_P$ provided by either the clerk C or the designated verifier ID_V. Now with this Aid, T computes $U_P = e(W_P, P)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_O} .U_o^n \right)^{-V_P}$ and $H_P = H_2(m, Aid)$. T accepts the signature if and only if $V_P = h\left(H_P, U_P\right)$.

5. ANALYSIS OF THE PROPOSED SCHEME

In this section first we discuss proof of correctness and then security analysis of the ID-DMPS scheme.

5.1 Proof of Correctness

The following equations give the proof of correctness for individual proxy signer’s signature.

$$\begin{aligned}
& e\left(W_{P_i}, P\right)\left(e\left(Q_{ID_O} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(W_{P_i}, P\right)\left(e\left(Q_{ID_o} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(V_P SKP_i + k_i P, P\right)\left(e\left(d_{ID_o} + d_{IDs_i}, P\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(V_P SKP_i, P\right) e\left(k_i P, P\right)\left(e\left(SKP_i - W_o + W_o - k_o P, P\right) U_o\right)^{-V_P} \\
& = e\left(SKP_i, P\right)^{V_P} e\left(P, P\right)^{k_i} e\left(SKP_i, P\right)^{-V_P} e\left(-k_o P, P\right)^{-V_P} U_o^{-V_P} \\
& = e\left(P, P\right)^{k_i} = U_{P_i}.
\end{aligned}$$

The following equations give the proof of correctness for multi-proxy signature.

$$\begin{aligned}
& e(W_P, P)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_o} .U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} W_{P_i}, P \right)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_o} U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} (V_P SKP_i + k_i P), P \right)\left(e\left(\sum_{i=1}^{n} \left(d_{ID_o} + d_{IDs_i} \right), P \right)^{V_o} U_o^n \right)^{-V_P} \\
& = \left(\sum_{i=1}^{n} (V_P SKP_i + k_i P), P \right)\left(e\left(\sum_{i=1}^{n} (SKP_i - W_o + W_o - k_o P), P \right) U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} SKP_i, P \right)^{V_P} \prod_{i=1}^{n} e\left(P, P\right)^{k_i} e\left(\sum_{i=1}^{n} SKP_i, P \right)^{-V_P} e\left(\sum_{i=1}^{n} -k_o P, P \right)^{-V_P} \left(U_o^n\right)^{-V_P} \\
& = \prod_{i=1}^{n} e\left(P, P\right)^{k_i} = U_P
\end{aligned}$$

5.2 Security Analysis

Our ID-DMPS scheme satisfies the following security requirements which are stated in section 3.2.

Strong Identifiability: Because identity pubic key Q_{IDs_i} of all proxy signers are involved in the verification of the proxy signature, anyone can identify all the proxy signers.

Strong Undeniability: The clerk verifies the individual proxy signature of each proxy signer, so no one can be deniable of his signature.

Distinguishability: This is obvious, because there is a warrant m_w in a valid multi-proxy signature, at the same time, this warrant m_w and the public keys of the original signer and the proxy signers must occur in the verification process.

Prevention of Misuse: Due to using the warrant m_ω, the proxy signers can only sign messages that have been authorized by the original signer.

Strong Unforgeability: In general, there are mainly three kinds of attacks: *outsiders*, who are not participating in the issue of the proxy signature; some *signers* who play an active in the signing protocol and the *user* (signature owner). Furthermore, some of these attackers might collude. The outsider-attack consists of the original signer attack and any third adversary attack. We assume that the third adversary can get the original signer's signature on warrant m_ω (So, our scheme needs not the secure channel for the delivery of the signed warrant). Even this, he forges the multi-proxy signature of the message $m^{'}$ for the proxy group *L* and the original signer, this is equivalent to forge a Hess's ID-based signature with some public key. On the other hand, the original signer cannot create a valid multi-proxy signature since each proxy key includes the private key d_{IDs_i} of each proxy signer.

In our scheme, the clerk is one of the proxy signers, but he has more power than other proxy signers. Assume that the clerk wants the proxy group to sign the false message $m^{'}$. He can change his U_{P_i} , therefore U_P can be changed, but from the security of the basic ID-based signature scheme and public one-way hash function H_2, it is impossible for the clerk to get $V_P^{'} \text{ and } W_P^{'}$ such that $\left\langle m, m_w, V_P, W_P, R_p, U_o \right\rangle$ is a valid multi-proxy signature. Also, the attack of some signers collude can be prevented for the identity of each proxy signer is involved in the verification of the signature.

Finally, the user can not forge the multi-proxy signature because he can not obtain more information than the Clerk.

Designated Verifiability: The designated verifier ID_V has to use his secret key d_{ID_V} at the time of verification of the multi-proxy signature. So, only the designated verifier can directly verify the validity of the proxy signature. No one can verify the validity of the multi-proxy signature without the help of either the designated verifier ID_V or the designated Clark.

5.3 Performance Analysis

Performance of signature scheme protocols can be approximated in terms of computation and communication overheads. In this section, we mainly discuss the performance of pro posed ID-DMPS scheme.

For convenience, the following notations are used to analyze the computation and communication complexity. T_{smul} represents the time for one scale multiplication in G_1, T_{pair} denotes the total one pairing computation; T_{mhash} define the time for one Map-to-Point hash function; N_t denotes the total number of transmissions and N_b denotes the total number of broadcasts. Note that the times for other computations or operations are ignored, since they are much smaller than T_{smul}, T_{pair} and T_{mhash}.

We summarize the computation and communication overheads of our proposed ID-DMPS scheme in Table1. As shown in Table1, The computation complexity for Setup, Extract, Generation of proxy key, Multi signature generation, Direct verification, Public verification algorithms are $1T_{smul}$, $(n+1)T_{smul}+(n+1)T_{mhash}$, $(2n+1)T_{pair} \quad +(2n+2)T_{mhash}+ (n+2)T_{smul}$, $4nT_{pair}+(3n+1)T_{mhash}+4nT_{smul}$, $3T_{pair}+2T_{mhash}$ and $2T_{pair}+2T_{mhash}$ respectively. Also the total communication overheads for generation of Proxy Key and Multi-Proxy signature generation algorithms are nN_t, nN_b+2nN_t respectively in our ID-DMPS scheme.

	Computation overheads	**Communication overheads**
System Setup	$1T_{smul}$	--
Key Extract	$(n+1)T_{smul}+(n+1)T_{mhash}$	--
Generation of proxy key	$(2n+1)T_{pair}+(2n+2)T_{mhash}+(n+2)T_{smul}$	nN_t
Multi-Proxy Signature Generation	$4nT_{pair}+(3n+1)T_{mhash}+4nT_{smul}$	nN_b+2nN_t
Multi-Proxy Direct Verification	$3T_{pair}+2T_{mhash}$	--
Multi-Proxy Public Verification	$2T_{pair}+2T_{mhash}$	--

TABLE 1: Computation and Communication Overheads for ID-DMPS Scheme

6. CONCLUSION

Proxy signature is an indispensable mechanism in the modern e-business and e-government infrastructures. Many variants of proxy signatures have been proposed in the literature. In this paper, we propose an ID-based directed multi-proxy signature scheme using bilinear pairings. This scheme allows only a designated verifier to directly verify the multi-proxy signature, generated by a group of proxy signers on behalf of the original signer, issued to him. In case of trouble or if necessary the designated verifier can prove the validity of the multi-proxy signature to any third party. Our scheme satisfies the security requirements such as strong identifiability, strong undeniability, distinguish ability, prevention of misuse of proxy signing power, strong unforgeability and designated verifiability. The proposed scheme is suitable for some applications where the signed message is personally or commercially sensitive to the signature receiver.

REFERENCES

[1] M. Mambo, K. Usuda, and E.Okamoto. "Proxy Signatures for Delegating Signing Operation". *In: 3rd ACM Conference on Computer and Communications Security(CCS'9),* pp.48-57, *New York,* ACM, 1996.

[2] C.L Hsu, T.S. Wu and T.C. Wu. "New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers". The Journal of Systems and Software, 58, pp.119-124, 2001.

[3] M.S.Hwang, I.C. Lin and J.L. Lu Eric. "A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers". International Journal of Informatica, 11(2), pp.1-8, 2000.

[4] H.M. Sun. “An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. Computer Communications, 22(8), 1999, pp.717-722.

[5] K. Zhang. “Threshold Proxy Signature Schemes”. Information Security Workshop, pp.191-197, Japan, 1997.

[6] J. Liu and S. Huang. “Identity-Based Threshold Proxy Signature from Bilinear Pairings”. Informatica, Inst. Math & Science, Vol. 21, No. 1, pp. 41-56, IOS press, 2010.

[7] S.J. Hwang, and C. H. Shi. “A Simple Multi-Proxy Signature Scheme”. Proceeding of the Tenth National Conference on Information Security, Taiwan, pp.134-138, Techinical report, 2000.

[8] X. Li, and K. Chen. “ID-based Multi-Proxy Signature, Proxy Multi-Signature and Multi-Proxy Multi-Signature Schemes from Bilinear Pairings”. Applied Mathematics Computation, Vol. 169, Issue 1, pp. 437-450, Elsevier, 2005.

[9] X. Li, K. Chen, and S. Li. “Multi-Proxy Signature and Proxy Multi-Signature Schemes from Bilinear Pairings”. Proceedings of PDCAT 2004*,* LNCS 3320, pp. 591–595, Springer-Verlag, 2004.

[10] L.Yi, G. Bai and G. Xiao. “Proxy Multi-Signature Scheme: A New Type of Proxy Signature Scheme”. Electronic Letters, Vol.36, No.6, pp.527-528, IEEE, 2000.

[11] S. Lal and A. K. Awasthi. “Proxy Blind Signature Scheme”. IACR, Cryptology e-print Archive*,*Report 2003/072, 2003. http://eprint.iacr.org.

[12] B. Majhi, D.K. Shau, and R.N. Subudhi. “An Efficient ID-Based Proxy Signature, Proxy Blind Signature and Proxy Partial Blind Signature”. International conference on Information Technology*,* pp. 19-23, IEEE, 2008.

[13] J.Hwang, and C. H. Chen. “A New Multi-Proxy Multi-Signature Scheme”, *2001* National Computer Symposium: Information Security, Taiwan, pp.19-26, 2001.

[14] X. Li, and K. Chen. “ID-based Multi-Proxy Signature, Proxy Multi-Signature and Multi-Proxy Multi-Signature Schemes from Bilinear Pairings”. Applied Mathematics Computation, Vol. 169, Issue 1, pp. 437-450, Elsevier, 2005.

[15] M. S. Hwang, S. F. Tzeng, S. F. Chiou. “An Ordered Multi-Proxy Multi- Signature Scheme”. Proceedings of the 8th International Conference on Intelligent Systems Design and Applications*,* Vol. 03, pp. 308-313, IEEE Computer Society, 2008.

[16] Y.Sun, C. Xu, F.Li, and Y.Yu. “Identity Based Multi-Proxy Multi-Signcryption Scheme for Electronic Commerce”. Proceedings of the5th International Conference on Information Assurance and Security, Vol.02, pp. 281-284, IEEE, 2009.

[17] Z. Xiaoyan, W.Yan, D .Wiefeng, and G. Yan. “An Improved ID-Based Multi-Proxy Multi-Signcryption Scheme”. Proceedings of the 2nd International Symposium on Electronic Commerce and Security, Vol.01, pp. 466-469, IEEE Computer Society, 2009.

[18] S.J Hwang and C.C. Chen. “Cryptanalysis of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. INFORMATICA, 14(2), pp.205-212, 2003.

[19] F. Li, Q. Xue, and Z. Cao “Bilinear pairings based designated-verifier multi-proxy signature scheme”, IT Revolutions, 2008 First Conference on, 2008.

[20] S. Lal and M. Kumar. “A directed signature scheme and its applications”. Proceedings of National conference on Information Security, pp. 124-132, New York, 8-9 Jan, 2003.

[21] R.Lu, X.Lim, Z.Cao, J.Shao and X.Liang, “New (t, n) threshold directed signatures schemes with provable security”, Information Sciences 178, pp.156-165,2008.

[22] X. Sun, Jian-hua Li, Gong-liang Chen, and Shu-tang Yung. “Identity-Based Directed Signature Scheme from Bilinear Pairings”. Cryptology eprint Archive, Report 2008/305, 2008. http:// *eprint.iacr.org.*

[23] B.Umaprasada Rao, P.Vasudeva Reddy, and T.Gowri. “An efficient ID-based DirectedSignature Scheme from Bilinear Pairings”. Cryptography e-print Archive Report 2009/617, Available at http://eprint.iacr.org.

[24] A. Shamir. “Identity-based cryptosystems and signature schemes”. Advances in Cryptology-Crypto 84, LNCS 196, Springer-Verlag, pp.47-53, 1984.

[25] D. Bonech and M. Franklin. “Identity Based Encryption from the Weil pairing”. Advance in CRYPTO’01, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[26] D. Boneh, B. Lynn, and H. Shacham. “Short signatures from the Weil pairing”. Advances in Cryptology-Asiacrypt’01, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

[27] J.C. Cha and J.H. Cheon. “An identity-based signature from gap Diffie-Hellman groups”. Public Key Cryptography 03, LNCS 2139, pp.18-30, Springer-Verlag, 2003,.

[28] F. Hess. “Efficient identity based signature schemes based on pairings”. SAC 02, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[29] F. Zhang and K. Kim. “ID-based blind signature and ring signature from pairings”. Advances in Cryptology-Asiacrypt 02, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.