ID-Based Directed Multi Proxy Chameleon Signature Scheme with Bilinear Pairing

Tejeshwari Thakurh

School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur(C.G.),India.

Abstract *— In this paper we first proposed an ID-based directed multi-proxy chameleon signature scheme using bilinear pairings. These schemes allow a group of proxy signers to make a valid proxy chameleon signature for a designated verifier. The designated verifiers only can easily such multi-proxy chameleon signatures generate on behalf of the original signer. Our proposed scheme is secure against existential forgery under adaptive chosen message attack assuming Computational Diffie-Hellman problem as a hard problem.*

Keywords *— Public Key Cryptography, Proxy Chameleon Signature, Bilinear Pairing.*

I. INTRODUCTION

Krawczyk and Rabin [9], introduced chameleon signature. It is in fact a signature based on hash and sign paradigm where chameleon hash function is a trapdoor collision resistant. Chameleon signatures provide non-repudiation and non-transferability for the signed message as the undeniable signatures [4] do, but chameleon signature allows simpler and more efficient realization than the undeniable signature. It is well known fact that chameleon hash function is used to determine the message digest.

The concept of proxy signature was introduced by Mambo et al.[14]. Proxy signature means electronics authentication in which the designated person can sign on behalf of the original signer. Since the invention of proxy signature, several type of proxy signatures have been designed. One among them is noteworthy proxy signature introduced by Hwang and Shi [8]. The advantage of this proxy signature lies with the fact that the original signer can delegate his signing power to many persons not only one. This type of signature scheme is known as multi proxy signature scheme. However, such multi proxy signature scheme fails to provide features like non-repudiation and non-transferability of the signed message. Since chameleon signature had the capacity to deal with such situation, Zhang et al.[19] utilized it to design proxy chameleon signature.

The concept of directed signature scheme was proposed by Lim and Lee [12]. In a directed signature scheme, any signature is generated for a designated verifier, who can directly verify the signature while others know nothing on its validity. In addition, at the time of trouble or if required, both the signer and the designated verifier can verify to a third party that the signature is valid. Later Yang et al. [18] extended it and made the directed proxy signature scheme. This scheme used the techniques of unforgeable under the Gap Diffie-Hellman Assumption.

Some multi proxy signatures with designated verifier are also given in the literature [11]. In these schemes, an original signer authorized a group of proxy signers and only with the cooperation of all these signers of the proxy group the proxy signatures could be generated for a designated verifier on behalf of the original signer. The designated verifier only can directly verify the multi-proxy signature issue to him. In these schemes, the designated verifier cannot convince any third party about the validity of the multi-proxy signatures scheme otherwise to solve this problem, it necessary to combine the concepts of multi proxy and directedness [10],[13],[16],[17] in order to design a signature.

The concept of ID-based cryptosystem is due to Shamir [15]. Such cryptosystem has the property that the identity information of each user works as his public key. ID-based cryptography has the advantage of easier key distribution as compared to conventional public key cryptography. Ateniese et al.[1],introduced the concept of ID-based chameleon hash function and in the case of chameleon hashing, the advantages of ID-based cryptography are multiplied by the reality that the owner of a public key does not necessarily need to recover the associated secret key. To the best of our knowledge there is no existing scheme with this concept having such intention we thus propose an ID-based directed multi proxy chameleon signature using chameleon hash function involving multi signers. Our proposed scheme is secure against existential forgery under adaptive chosen message attack in the random oracle model assuming Computational Diffie-Hellman problem and maintains the security at par with Zheng et al.[19] in the case of multi signers.

The organization of rest of the paper is as follows:
The required preliminaries for proposed design are given in section 2. In section 3, discussion of the design algorithm is given with notations and definitions. The proposed identity-based directed multi proxy chameleon signature is given in section 4. Further an analysis of proposed scheme is described in section 5. In section 6, the security and efficiency aspects of proposed scheme are discussed. Finally, the conclusion of proposed design is given in section 7.

II. PRELIMINARIES

First we describe bilinear pairings and Gap Diffie-Hellman group respectively. Next, we present ID-based public key setting for bilinear pairings.

A. Bilinear Pairing

Let G_1 be a cyclic additive group generated by *P*, whose order is a prime *q*, and G_2 be a cyclic multiplicative group of the same order *q*. Let *a* and *b* be the elements of Z_q^*. We assume that the discrete logarithm problems (DLP) in both the groups G_1 and G_2 are hard. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

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

B. Gap Diffie-Hellman Group

Let G_1 be a cyclic additive group generated by *P*, whose order is a prime q. Assume that the inversion and multiplication in G_1 can be computed efficiently. We first introduce following problems in G_1:

- Discrete Logarithm Problem (DLP): Given two elements *P* and *Q*, to find an integer $n \in Z_q^*$, such that *Q* = *nP* whenever such an integer exists.
- Computation Diffie-Hellman Problem (CDHP): Given *P*, *aP*, *bP* for $a, b \in Z_q^*$, to compute *abP*.
- Decision Diffie-Hellman Problem (DDHP): Given *P*, *aP*, *bP*, *cP* for $a, b, c \in Z_q^*$ to decide whether $c \equiv ab \bmod q$.

We call G_1 a Gap Diffie-Hellman Group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP or DLP with non negligible probability. Such group can be found in super singular elliptic curve or hyper elliptic curve over finite field, and bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [2,6, 7].

III. NOTATIONS AND THE ALGORITHM FOR PROPOSED SCHEME:

Next we recall notations given in [3,19,20] as below:

Symbol	Description
G_1	Cyclic additive group
G_2	Cyclic multiplicative group
q	Prime Number
e	Bilinear Map
a,b	Integer number
P and *Q*	Generator of group G
H	Secure hash function
r	Random Number
SK	Secret key
PK	Public Key
m	Message
σ	Signature
w	Warrant
ID	Identity
‖	Concatation

Table 1.

A. ID-based Direct Multi Proxy Chameleon Signature Scheme

An ID-based directed multi proxy chameleon signature scheme consists of four entities: original signer, proxy signer group, designer verifier and other party as in charge called Judge who will watch the communication between proxy group and the designer verifier. We define the algorithm for ID-based directed multi proxy chameleon signatures as below:

a). Setup:- The private key generator (PKG) runs probabilistic polynomial-time algorithm to generate a pair of keys *(SK; PK)* defining the scheme. PKG publishes the system parameters of *SP* including the public key *PK*, and keeps the master key *SK* secret. The input to this algorithm is a security parameter 1^k.

b). Extract:- A deterministic polynomial-time algorithm that, on input the master key *SK* and an identity string *ID*, outputs the trapdoor key associated to the hash key S_{ID}.

c). Generation of the Proxy Key:- This is a protocol between the original signer and all multi proxy signers. The protocol works as follows: The proxy signers take as input their private keys, S_A on ID_A, and the delegation warrant m_w which includes the type of the information delegated. The original signer uses public key and the warrant mw with respect to proxy group whose proxy signers sign as the proxy signing key SK_{P_i} so that original signer and the proxy signer produce proxy chameleon signature on behalf of the original signer.

d). Chameleon Hash Function:- A probabilistic polynomial-time algorithm that, on input an identity string *ID*, message *m*, and a random string *R*, outputs the hashed value *h = Hash(ID, PK, m, R).*

e). Forge:- A deterministic polynomial - time algorithm *F* that, on input *PK* the trapdoor key S_{ID} associated to the identity string *ID*, a hash value h of a message *m*, a random string *R*, and another message $m' \neq m$, outputs a string *R* that satisfies *h = Hash(ID, PK, m, R) =Hash(ID, PK, m', R').*

f). Dispute:- Given directed multi proxy chameleon signature σ_{DMPCS} on message *m*, the proxy group computes different message *m'* and *R'*, collision as pair *(m', R')*, where $m' \neq m$ and with the valid signature tuple (m', R', σ_{DMPCS}), the Judge claim that ID-based directed multi proxy chameleon signature of message *m'* is forgery.

B. Security Model

In this section, we give security requirement of the proposed scheme based on [5, 19]: satisfying following properties:

Strength:

Distinguishability: Valid directed multi proxy chameleon signatures generated by the proxy signers are distinguishable from valid normal chameleon signatures generated by the original signer.

- ***Verifiability:*** From the directed multi proxy chameleon signature, a verifier can be convinced of the original signer's contract on the signed message.
- ***Unforgeability:*** Only the delegated proxy group can generate the proxy signature for a given message on behalf of the original signer. The other party and the original signer not designated as a proxy signer cannot produce a proper chameleon signature which is not generated by the signer earlier.
- ***Identifiability:*** Any one can identify the proxy signer corresponding to a directed multi proxy chameleon signature.
- ***Prevention of misuse:*** The proxy signer's cannot use the proxy key for the purpose other than generating a valid directed multi proxy chameleon signature. The other person cannot sign, with the proxy key, the messages which have been not authorized by the authentic signer.
- ***Designated Verifiability:*** The designated verifier uses their secret key to verify the directed multi proxy chameleon signature generated by a proxy signer's on behalf of the original signer. So the only designated verifier can verify the proxy signature issued to him.
- ***Non-Repudiation:*** Once a directed multi proxy signer creates a valid directed multi proxy chameleon signature of an original signer, he can't accept the signature creation.
- ***Non-Transferability:*** Except for the proxy signers himself, no one can prove to another party that the proxy signer's produced a given directed multi proxy chameleon signature.
- ***Denial:*** The proxy signers can convince the judge to reject a forgery proxy chameleon signature.
- ***Message Hiding:*** In case of dispute, the proxy signers can compute a new denial the forgery proxy chameleon signature and thus the original message is never revealed.

IV. THE PROPOSED SCHEME

The proposed scheme involves four characters: The Private Key Generator (PKG), the original signer, group of proxy signers $PS_i = PS_1, PS_2 \ldots\ldots\ldots PS_l$ and the recipient. We propose a ID-based directed multi proxy chameleon signature scheme consists of following phases:

1. ***Setup:*** Let G_1 is a cyclic additive group generated by *P* with prime order *q*. G_2 is a cyclic multiplicative group of the same order *q*. $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing $H_0 : \{0,1\}^* \rightarrow G_1, H_1 : \{0,1\}^* \rightarrow Z_q^*$ and $H_2 : G_2 \times G_1 \rightarrow Z_q^*$ cryptography hash function and $P_{Pub} = sP$. PKG publishes system parameters $\{G_1, G_2, e.q, P, P_{Pub}, H_0, H_1, H_2\}$.Here PKG keeps *s* as the master-key (Private).

2. ***Extract:*** Let Alice be the original signer with identity ID_A, private key be the $S_A = sQ_{ID_A} = sH_0(ID_A),(PS_i)$ be the proxy signers with identity ID_{PS_i} and customized identity: $ID_j = (ID_{recipient} \| ID_{\text{Proxysigner}} \| ID_{transaction})$, where the identity of the recipient, proxy signer, transaction, and the private key $(S_{PS_i}) = sQ_{PS_i} = sH_0(ID_{PS_i})$.

3. ***Proxy Key Generation:*** To delegate the signing capacity to proxy signers, the original signer uses Hesss ID-based signature scheme [7] to generate the signed warrant m_w and each proxy signer PS_i computes his proxy key S_{P_i}.

-Alice computes $r_A = e(P,P)^k$, where $k \in_R Z_q^*$, and computes $c_A = H_2(m_w \| ID_A \| r_A)$ and $U_A = c_A S_A + kP$. Then Alice sends (m_w, c_A, U_A) to the proxy group L.

- Each PS_i verifies the validity of the signature on m_w and computes $r_A = e(U_A, P)e(Q_A, P_{Pub})^{-c_A}$ then accepts this signature if and only if $c_A = H_2(m_w \| ID_A \| r_A)$. If the signature is valid, PS_i computes the proxy key S_{P_i} as $S_{P_i} = c_A S_{PS_i} + U_A$.

4. ***Directed Multi Proxy Chameleon Signature Generation***:

-Hash: Given a message $m \in \{0,1\}$, each PS_i choose a random element R from G_1 and calculate the chameleon hash:

$h = Hash(P_{pub}, m, R, ID_j) = e(R, P)e(H_1(m)H_0(ID_j), P_{pub})$

- Forge: Recipient can make a forgery:

$R = Forge(P_{pub}, ID_j, S_j, m, R, m') = (H_1(m) - H_1(m')Q_j + R)$,

and accepts this signature if and only if $c_p = H_2(h \| ID_j \| r_p)$. The proxy group L wants to sign a delegated message m on behalf of the original signer. Each proxy signer PS_i generates the partial proxy signature to generate directed multi proxy signature.

-Each: PS_i randomly selects an integer $k_i, k_j \in_R Z_q^*$, compute $r_{P_i} = e(P, P)^{k_i}$, $L_{P_i} = e(S_{PS_i}, Q_v)^{k_j}$ and broadcasts r_{p_i}, L_{p_i} to the remaining $l-1$proxy singers. Then compute

$$r_p = \prod_{i=1}^{l} r_{p_i} \quad \text{and} \quad L_p = \prod_{i=1}^{l} L_{p_i}$$

and $U_{P_i} = c_p S_{P_i} + k_{P_i} P$. Finally, the individual proxy signature of the message m is (c_p, U_{p_i}).

and $c_p = H_2(h \| ID_j \| r_p)$. Once all individual proxy chameleon signatures are correct, then thus computes

$$U_p = \prod_{i=1}^{l} U_{p_i}$$

The valid directed multi-proxy chameleon signature is therefore the tuple: $< m, R, c_p, U_p, m_w, r_A >$.

5. ***Verification:*** Verification phase is divided into two parts as described on our scheme. First is direct verification and other is the public verification.

(A) Direct verification: Given identity *ID*, the designated verifier *v* first calculate

$r_p = e(U_p, P)(e(\sum_{i=1}^{l}(Q_A + Q_{PS_i}), P_{pub})^{c_A}, r_A^l)^{-c_A}$

and accepts the signature if and only if $c_p = H_2(h \| ID_j \| r_p)$.

(B)Public Verification: Given a signature $< m, R, c_p, U_p, m_w, r_A >$ on signer ID_s, verifier ID_v and message *m*, to enable third party *J* to verify it either signer and verifier *ID* compute $Aid = L_p$ provide by either the employees or designated verifier *ID*. Now with this *Aid*, *J* compute

$r_p = e(U_p, P)(e(\sum_{i=1}^{l}(Q_A + Q_{PS_i}), P_{pub})^{c_A} \cdot r_A^l)^{-c_p}$.

J accepts the signature if and only if $c_p = H_2(h \| ID_j, \| r_p)$.

Dispute: In the case of dispute up on the validity of the signature the following case arises: to generate collision in the chameleon hash function, for a given forgery $(m', R', c_p, U_p, m_w, r_A)$, the recipient employee uses to compute the multi proxy chameleon signature up on original message *m*.

Input: The process is

$Hash(P_{pub}, m, R, ID_j) = Hash(P_{pub}, , m', R', ID_j)$

where $m' \neq m$ and proxy signers calculate $t = \frac{R'-R}{H_1(m) - H_1(m')}$.

- Proxy signers choose any message $\tilde{m}$ and computes $\tilde{R} = (H_1(m) - H_1(m')Q_j + R)$

Output: Output is $(\tilde{m}, \tilde{R})$ with the tuple $(\tilde{m}, \tilde{R}, c_p, U_p, m_w, r_A)$, proxy signer can convince the judge *J* to reject the false proxy chameleon signature $(m', R', c_p, U_p, m_w, r_A)$.

-Judge *J* applies the above verification algorithm. If this verification fails then the alleged signature is rejected by *J*, Otherwise;

- *J* summons the proxy signer to deny/accept the signature.

V. CORRECTNESS OF THE PROPOSED SCHEME

The correctness of the signature is justified by the following equations: chameleon signature and ID-based directed multi proxy chameleon signature have the same algorithm for chameleon hashing. Therefore the following proofs of correctness owes much to the [7,20]. The forgery equation is.

$$\begin{aligned}
&Hash(P_{pub}, m', R', ID_j) \\
&= e(R', P)e(H_1(m')H_0(ID_j), P_{pub}) \\
&= e((H_1(m) - H_1(m')Q_j + R), P)e(H_1(m')Q_j, P_{pub}) \\
&= e(H_1(m) - H_1(m')Q_j, P)e(R, P)e(H_1(m')Q_j, P_{pub}) \\
&= e(R, P)e(H_1(m) - H_1(m')Q_j, P)e(H_1(m')Q_j, P_{pub}) \\
&= e(R, P)e(H_1(m) - H_1(m')H_0(ID_j), P_{pub})e(H_1(m')H_0(ID_j), P_{pub}) \\
&= e(R, P)e(H_1(m)H_0(ID_j), P_{pub}) \\
&= Hash(P_{pub}, m, R, ID_j)
\end{aligned}$$

Verifiability: The verification and correctness of the ID-based directed multi proxy chameleon signature is justified by the equation:

$$e(U_p,P)(e(\sum_{i=1}^{l}(Q_A+Q_{PS_i}),P_{pub})^{c_A}\cdot r_A^l)^{-c_p}$$

$$= e(\sum_{i=1}^{l}U_{p_i},P)e(\sum_{i=1}^{l}(S_A+S_{PS_i}),P)^{c_A}\cdot r_A^l)^{-c_P}$$

$$= e(\sum_{i=1}^{l}U_{p_i},P)e(\sum_{i=1}^{l}(S_{p_i}-kP,P)\cdot r_A^l)^{-c_P}$$

$$= e(\sum_{i=1}^{l}c_pS_{p_i}+k_{p_i}P,P)e(\sum_{i=1}^{l}(S_{p_i},P))^{-c_P}$$

$$= e(\sum_{i=1}^{l}k_{p_i}P,P)$$

$$= \prod_{i=1}^{l}r_{p_i}$$

$$= r_P$$

VI. Security Analysis of Proposed Scheme

Theorem 1. The proposed ID-based directed multi proxy chameleon signature scheme enjoys all advantages of proxy signature schemes [19] i.e Distinguishing ability, Verifiability, Identifiability, Prevention of misuse, Non-forge ability, Designated verifiability, non-repudiation, Non-transferability, Denial and Message hiding.

Proof. Distinguishability: It is evident that the valid ID-based directed multi-proxy chameleon signatures are distinguishable from normal valid multi proxy chameleon signatures generated by anyone.

Verifiability: The verifier can be made convinced that the proxy signers have the original signers signature on the warrant mw and warrant contain identity information and delegated signing capacity to verify, with the verification tuple (m,R,c_P,U_P,m_w,r_A) from the construction of $(c_P,U_P,,r_A)$ in directed multi proxy chameleon signature verification scheme.

Non-forgeability: The proxy group can generate the ID-based directed multi proxy chameleon signature for a given message *m'* and the original signer is signature on warrant m_w. Even if some adversary wants to forge the multi-proxy signature of the message *m'* for the proxy group and the original signer Alice. But he cannot forge this signature, since our scheme is based on Hess's [7], ID-based signature scheme, which is proved to be secure against existential forgery on adaptive chosen message attacks under the random oracle model assuming CDH Problem is hard. On the other hand, the original signer cannot create a valid directed multi-proxy signature since each proxy key includes the private key SP_i of each proxy signer. Assume that the adversary wants the proxy group to sign the false message *m'*. He can change his r_{P_i} , therefore *rP* can be changed, but from the security of the basic ID-based signature scheme and public one way hash function H1, it is impossible for the adversary to get c'_P and U'_P such that $<m',c'_p,U'_P,m_w,r_A>$ is a valid ID-based directed multi-proxy chameleon signature.

Identifiability: The identities of public key of all proxy signers are involved in the verification of the ID-based directed multi proxy chameleon signature. Therefore any one can identify all the proxy chameleon signatures.

Prevention of Misuse: An ID-based directed multi proxy chameleon signature scheme due to use of the warrant m_w, the proxy group can sign message only that have been authorized by the original signer, nothing else.

Designated Verifiability: The designated verifier *v* on *ID* has to use his secret key sQ_A at the time of verification of the directed multi-proxy signature. So, the only designated verifier can directly verify the validity of the proxy signature. No one can verify the validity of the ID-based directed multi-proxy signature without the help of either the designated verifier *v* on *ID* or the designated employees.

Non-repudiation: The proxy signers generated by valid ID-based directed multi proxy chameleon signature can generate (m,R,c_p,U_P,m_wr_A), but those proxy signers cannot generate other signature (m',R',c_p,U_P,m_wr_A) , where $m'\neq m$. This is equivalent to finding a collision of the Id-based chameleon hash function, assuming CDHP hard.

Non-Transferability: Proxy signers generate ID-based directed multi proxy chameleon signature for recipient and compute a random value on message m then the equation $R'=(H_1(m)-H_1(m')Q_j+R)$ and $Hash(P_{pub},m,R,ID_j)=Hash(P_{pub},m',R'ID_j)$ has the hash value. Hence our ID-based directed multi proxy chameleon signature verify the correct value is (m',R',c_p,U_P,m_wr_A) . Thus we see that the recipient can not the convince a third party because *m'* have exactly one value *R'*. *R'* produces proper signature tuple which is nothing efficient computation.

Denial: In the proposed scheme the proxy signers can convince the judge to reject a forgery directed multi proxy chameleon signature i.e proxy signers and the recipient can give the authority to judge *J* from recipient signature $(\tilde{m},\tilde{R},c_p,U_P,m_w,r_A)$. If any proxy signer wants to claim that the signature is invalid, he needs to provide a collision in the hash function, the value $m'\neq m$ and a value *R'* such that $Hash(P_{pub},ID_j,\tilde{m},\tilde{R})=Hash(P_{pub},ID_j,m,R)$

In this case the ID-based directed multi proxy chameleon signature σ_{DMPCS} is originally generated by proxy signers with the pair $(m, R) \neq (\tilde{m}, \tilde{R})$.

Message Hiding: During, the message hiding process in ID-based directed multi proxy chameleon signature, the original signer constructs another false signature for any message with the same element of directed multi proxy chameleon signature. Original signer do not disclose the original message.

Key Exposure Freeness

As per the algorithm given in [1,9] If a recipient with identity ID_c has never computed a collision under a customized identity ID_j, then there is no efficient method for an adversary to find a collision for a given chameleon hash value in *DMPCS* other then $Hash(P_{pub}, ID_j, m, R)$. This must remain true even if the adversary has oracle access to *F* and is permitted polynomial many queries on triples (ID_j, m_j, R_j) of his choice, except that ID_j is not allowed to equal the challenge *ID*.

A. ***Efficiency***

The proposed scheme has computational cost abbreviated as follows:

Notation	Definition
$MulG_2$	Multiplication in the group
Mul	Multiplication
H_1 and H_2	Hash function
Exp	Exponent
M_2P	Map -to-Point
Add	Addition
Pa	Pairing
Sum	Summation

Table 2.

Phase	Set - up	Extract	Key Gen.	Sig. Gen.	Directed verify	Pub. verify
H_1			2	1		
H_2				1		
Exp			2		3	3
M_2P		2		1		
Mul	1		3	3		
Add			2	1	1	1
$MulG_2$			1	1	1	1
Pa			2	3	1	1
Sum			1		1	1

Table 3.

As per above table, to view the efficiency of proposed scheme during different phases the cost is estimated as below:

- The setup phase is *1Mul*
- Extract phase is $2M_2P$

-Key generation is

$2H_1 + 2Exp + 3Mul + 12Add + 1Mul + 2Pa + 1Sum$

- Signature generation is

$1H_1 + 1H_2 + 1M_2P + 3Mul + 1Add + 1MulG_2 + 2Pa$

-Verification is $3Exp + 1Add + 1MulG_2 + 2Pa + 1Sum$

VII. CONCLUSIONS

We first proposed an ID-based direct multi proxy chameleon signature scheme with bilinear pairing scheme. Our scheme is based on Hess's [7] scheme, which is more secure against existential forgery under adaptive chosen message attack in the random oracle model. So we can see that our scheme is secure from existential forgery attack, using Computational Diffie-Hellman problem.

ACKNOWLEDGMENT

The author is thankful to UGC, New Delhi, India for providing Rajiv Gandhi National fellowship (F1-17.1/2010-13/RGNF-2012-13-ST-CHH-35416) as financial assistance for this Research work.

REFERENCES

[1] G. Ateniese, B. de Medeiros, Identity-based chameleon hash and applications, *FC 2004*, *LNCS 3110*, *Springer-Verlag*, pp.164-180,2004.

[2] D. Boneh ,M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology 01*, LNCS 2139, Springer-Verlag, pp.213-229,2001.

[3] A. Boldyreva, A. Palacio, and B. Warinschi, Secure proxy signature schemes for delegation of signing rights, http:// venona.antioffline.com/2003/096.

[4] D. Chaum and H. van Antwerpen, Undeniable signatures, *Advances in Cryptology-Crypto* 1989, LNCS 435, Springer-Verlag, pp.212-216,1989.

[5] S. Goldwasser, S. Micali, R. Rivest, A digital signature scheme secure against adaptative chosen- message attacks, *SIAM Journal of Computing*, 17(2) , pp:281-308,1988.

[6] S.D. Galbraith, K. Harrison, D. Soldera, Implementing the Tate pairings, *ANTS 02*, LNCS 2369, Springer-Verlag, pp.324-337,2002.

[7] F. Hess, Efficient identity based signature schemes based on pairings, *SAC 02*, LNCS 2595, Springer-Verlag, pp. 310-24,2002.

[8] S.J. Hwang, and C. H. Shi. A Simple Multi- Proxy Signature Scheme. Proceeding of the Tenth National Conference on information Security, Taiwan, pp. 134-138,2000.

[9] H. Krawczyk, T. Rabin. Chameleon hashing and signatures, Proc. of NDSS 2000 , pp.143-154.

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

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

[12] C.H. Lim, P.J. Lee, Modified Maurer-Yacobis scheme and its applications, *Advances in Cryptology* -AUSCRYPT92, LNCS 718, Springer-Verlag, , pp. 308-323,1992.

[13] 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.

[14] M. Mambo, K. Usuda, E. Okamoto, Proxy signature, Delegation of the power to sign messages, In *IEICE Trans.Fundamentals*, E79-A, pp.1338-1353,1996.

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

[16] 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.

[17] B. Rao, P. Reddy, and T. Gowri. An efficient ID-based Directed Signature Scheme from Bilinear Pairings. *Cryptography e-print Archive Report* 2009/617, Available at http://eprint.iacr.org.

[18] M. Yang, W. Yu-min, Directed Proxy Signature in the Standard Model, *J. Shanghai Jiaotong Univ. (Sci.)* 16(6), pp. 663-671,2011.

[19] M. Zhang, G.Chen,J. Li, E_cient ID-based Proxy Chameleon Signature from Bilinear Pairings, *Computer and Computational Sciences*, IMSCCS '06. First International Multi-symposiums,pp. 135-141,2006.

[20] F. Zhang, R. Safavi-Naini, and W. Susilo. ID-based chameleon hashes from bilinear pairings, available at Cryptology ePrint Archive: Report 2003/208, 2003.