Int. J. Adv. Res. Sci. Technol. Volume 5, Issue 2, 2016, pp.571-576.

IJARST

International Journal of Advanced Research in Science and Technology

journal homepage: www.ijarst.com

ISSN 2319 – 1783 (Print)

ISSN 2320 – 1126 (Online)

ID-Based Directed Blind Signature Scheme from Bilinear Pairings.

Umaprasada Rao B.[1]* and Vasudeva Reddy P.[2]

[1]*Department of Engg Mathematics, Dr L B College of Engg. for Women, Visakhapatnam, India.*
[2]*Department of Engg Mathematics, AU college of Engineering, Andhra University, Visakhapatnam, A.P, India.*

**Corresponding Author's Email: umaprasadcrypto@yahoo.com*

A R T I C L E I N F O

Article history:

Received : 08 Apr. 2016
Accepted : 06 May. 2016
Available online : 31 May. 2016

Keywords:

Blind signature scheme,
Bilinear pairing,
CDH problem,
Directed Signature Scheme,
Hess ID based digital signature scheme,
Identity-based Cryptography.

A B S T R A C T

Blind signature, introduced by Chaum, allows a user to obtain a signature on a message without revealing anything about the message to the signer. Blind signatures play an important role in plenty of applications such as e-voting, e-cash system where anonymity is of great concern. Identity based (ID-based) public key cryptography can be a good alternative for certified based public key setting, especially when efficient key management and moderate security are required. In this paper, we propose an ID-based directed blind signature scheme (ID-DBS) from bilinear pairings, which combines the concepts of blind signatures and directed signatures. The proposed ID-DBS scheme allows a user to obtain a signature on a message without revealing anything about the message to the signer; and sends it to the designated verifier. The designated verifier can only verify the validity of the signature and in case of trouble or if necessary he can prove the validity of the signature to any other party. The proposed scheme is based on the Hess ID-based digital signature scheme. Finally, we discuss the correctness and security of the proposed ID-DBS scheme.

PAPER-QR CODE

IJARST Volume 5, Issue 1

Citation: *Umaprasada. et. al., ID-Based Directed Blind Signature Scheme from Bilinear Pairings, Int. J. Adv. Res. Sci. Technol. Volume 5, Issue 2, 2016, pp.571-576.*

Introduction:

Digital signature is a cryptographic tool to authenticate electronic communications. Digital signature scheme allows a user with a public key and a corresponding private key to sign a document in such a way that anyone can verify the signature on the document (using her/his public key), but no one can forge the signature on any other document. This self-authentication is required for some applications of digital signatures such as certification by some authority. In many situations, signed message is sensitive to the signature receiver. Signatures on medical records, true information and most personal or business transactions are such situations. Consider with a user A wants to generate a signature on a message m, sensitive for B and the message is also of concern to other users. For this situation, the form of the signature should be such that only B can directly verify the signature and that B can prove its validity to any third party C, whenever necessary. Such signatures are called directed signatures [4,5,11,12,13]. In a directed signature scheme, the signature receiver B has full control over the signature verification process. Nobody can check the validity of signature without his operation.

The concept of directed signatures was first presented by C.H.Lim and P.J.Lee [12] based on GQ signature scheme [7]. Directed signature schemes based on Schnorr signature [19], RSA signature scheme[18] also have been proposed [9, 10]. Recently, many variants of directed signature schemes have been proposed in the literature [22, 23, 24].

Blind signature is one of the variant of digital signature scheme, plays a central role in cryptographic protocols such as e-voting, e-payment that require user anonymity. A user can obtain from a bank a digital coin using a blind signature protocol. The coin is essentially a token properly signed by the bank. The blind

signature protocols enable a user to obtain a signature from a signer so that the signer does not learn any information about the message it signed and so that the user cannot obtain more than one valid signature after one interaction with the signer. The concept of blind signatures provides anonymity of users in applications such as electronic voting, electronic payment systems etc.

The concept of a blind signature scheme was introduced by Chaum [6] in 1982. A blind signature scheme allows a user to acquire a signature from the signer without revealing message content for personal privacy. The basic idea is as follows. The user chooses some random factors and embeds them into the message to be signed, while the signer cannot recover the message. Using the blind signature scheme, the user gets the blinded signature and removes the random factors. Then the user outputs a valid signature. This property is very important for implementing e-voting, e-commerce, and e-payment systems, etc. Many blind signature schemes, using traditional PKI, have been proposed in the literature [14, 16, 17, 20].

In traditional PKI, the public key is a random string that is unrelated to the identity of the user. Thus, a trusted authority is needed to assure the relationship between public key and the user by producing a certificate, which results in complex certificate management. Thus, the certificate management, including revocation, storage, distribution, and the computational cost of certification verification are the main difficulties against traditional PKI.

To overcome the difficulties mentioned above in traditional PKI, Shamir [21] introduced the concept of identity-based cryptography in 1984. The idea of IBC is to get rid of certificates by allowing a user's public key to be any binary string that uniquely identifies the user. Examples of such strings including e-mail addresses and IP address. The private key of a user is produced by a trusted party called a private key generator (PKG), with the help of the PKG's master secret key. Thus it can simplify certificate and key management in traditional public key system.

Several Practical Identity based signature schemes have been proposed since 1984, but a satisfying IBE scheme only appeared in 2001 [1]. It was devised by Boneh and Franklin and cleverly uses bilinear maps (Weil or Tate pairing) over super singular elliptic curves. In 2002, Paterson proposed and IBS from pairings on elliptic curves [15]. But no formal proof for the security was not presented in [15].

In 2003, Hess [8] proposed efficient IBS scheme based on pairings. In the same year 2003, Cha and Cheon [3] presented another IBS scheme from the Gap Diffie-Hellman Groups. They proved that their schemes are secure against existential forgery under adaptive chosen message and fixed ID-attack in the random oracle model with the assumption that the CDH problem is intractable. The proofs are obtained through pointcheval and Stern forking lemma. In 2005, Barreto and Libert [2] proposed efficient and provable secure identity based signature scheme from bilinear pairings.

In many situations, signed message is sensitive to the receiver and also a user acquire a signature from the signer without reveling message content for personal privacy. To fulfill this requirement in this paper, we propose an "ID-based Directed Blind Signature Scheme from Bilinear Pairings" which combining the concept of blind signatures and digital signatures. To the best of our knowledge our scheme is the first ID-based Directed Blind Signature Scheme using pairings. We use Hess's ID-based signature scheme [8] as the base for our scheme. The proposed scheme is validated and its security is proven under the assumption that the hardness of the Computational Diffie-Hellman Problem.

The rest of the paper is organized as follows. In Section 2 briefly explains the bilinear pairings and some computational problems on which our scheme is based. In Section 3, syntax and security requirements of the proposed scheme is described. Our proposed scheme is depicted in Section4. Proof of correctness and security analysis of the proposed scheme is presented in Section5. Finally Section6 concludes this paper.

Preliminaries:

In this section, we will briefly review the basic concepts on bilinear pairings and some related mathematical problems. We also present ID-based public key setting from pairings.

Bilinear Pairings:

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 $P, Q \in G_1$.

Computational problems:

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

Discrete Logarithm Problem (DLP):

Given two group elements P and Q, find an integer n such that $Q = nP$ whenever such an integer exists.

Decisional Diffie-Hellman Problem (DDHP):

For $a,b,c \in_R Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.

Computational Diffie-Hellman Problem (CDHP):

For $a,b,c \in_R Z_q^*$, given P, aP, bP, Compute abP.

We assume through this paper that CDHP and DLP are intractable. When the DDHP is easy but the CDHP is hard on the group G_1, we call G_1 a Gap Diffe-Hellman (GDH) group. Such groups can be found on super singular elliptic curves or hyper elliptic curves over finite field and the bilinear pairings can be derived from the Weil or Tate pairing.

Review of Hess-ID- based signature scheme:

To prepare for our ID-DS scheme, we use the following Hess ID-based signature scheme [8] given by Hess as the base scheme.

System Setup:

For a given security parameter l, the PKG chooses two groups G_1, G_2 of prime order $q \geq 2^l$ with a bilinear pairing e and a generator $P \in G_1$, as described in 2.3.1. He then selects $s \in_R Z_q^*$ randomly and computes the public key $P_{pub} = sP$, also picks a hash function $H_1 : \{0,1\}^* \rightarrow G_1^*$ and another cryptographic hash function $h : \{0,1\}^* \times G_2 \rightarrow Z_q^*$. The PKG now publishes system parameters as $params < G_1, G_2, e, P, P_{pub}, H_1, h >$ and keeps $< s >$ secret as master key.

Key Extract:

For a given user's identity $ID \in \{0,1\}^*$, the PKG computes $Q_{ID} = H_1(ID) \in G_1$, and $d_{ID} = sQ_{ID} \in G_1$. PKG returns d_{ID} as user's private key.

Signature Generation:

To sign a message $M \in \{0,1\}^*$, using the secret key d_{ID}, the signer chooses an arbitrary $P_1 \in G_1$ and picks a random integer $k \in z_q^*$. Then signer computes

$$R = \hat{e}(P_1, P)^k,$$
$$V = h(M, R),$$
$$U = Vd_{ID} + kP_1.$$

The signature on message *M* is $\sigma = (U, V) \in G_1 \times Z_q^*$.

Signature Verification:

On receiving a message *M* and signature $\sigma = (U,V)$, the verifier computes

1. $R = e(U, P)\, e(Q_{ID}, -P_{pub})^V$,
2. Accept the signature if and only if $V = h(M, R)$.

Syntax and Security Requirements of Blind Signature Scheme:

The formal definition of a blind signature is presented below.

Blind Signatures:

A blind signature scheme consists of three algorithms and two parties (the user and the signer). The details are as follows.

System Key Generation:

This is a probabilistic polynomial time algorithm (PPT algorithm). It takes a security parameter *k* as its input and outputs a pair of public key and private key *{y, x}* for the blind signature scheme, where *x* is preserved secretly by the signer.

Generation of Blind Signatures:

This is an interactive and probabilistic polynomial time protocol, which is operated by the user and the signer. The user first blinds the message *m* and obtains a new version m' of *m*, and then sends it to the signer. The latter utilizes her private key to sign on m' and obtains S', and then sends it to the sender. The sender unblinds it to obtain S which is a blind signature on *m*.

Verification of Blind Signatures:

This is a deterministic polynomial time algorithm. Given a message *m* and its alleged blind signature S, anyone who knows the public key *can* verify the validity of S. If it is valid, then the algorithm outputs '1'; otherwise outputs '0'.

The blind ness property of a signature scheme may be formally defined as follows: A blind signature scheme possesses the blindness property, if the signer's view (m', S') and the message-signature pair (m, S) are statistically independent. A secure blind signature scheme must satisfy the following three requirements:

Correctness:

If the user and the signer both comply with the algorithm of blind signature generation, then the blind signature S will be always accepted.

Unforgeability of Valid Blind Signatures:

It is with respect to the user especially, i.e. the user is not able to forge blind signatures which are accepted by the algorithm of Verification of Blind Signatures.

Blindness:

While correctly operating one instance of the blind signature scheme, let the output be (*m, S*) (i.e. message signature pair), and the view of the protocol V^1. At a later time, the signer is not able to link V^1 *to* (*m, S*).

Proposed ID-based Directed Blind Signature Scheme:

In this section, we present an ID-based Directed Blind Signature Scheme from the Bilinear Pairings.

Setup:

The PKG chooses $s \in Z_q^*$ as his master key and computes the global public key P_{pub} as sP. PKG also selects a map-to-point hash functions $H_1, H_2: \{0,1\}^* \rightarrow G_1^*$ and another cryptographic hash function$h$: $\{0,1\}^* \times G_2 \rightarrow Z_q^*$. PKG publishes system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, H_2, h >$ and keeps the master key $< s >$ as secret.

Extract:

Given signer's public identity $ID \in \{0,1\}^*$ compute the public key $Q_{ID} = H_1(ID)$ and the private key $d_{ID} = sQ_{ID}$.

Blinding Signature Protocol:

Given a signer's private key $d_{IDs}$and a message $m \in \{0,1\}^*$

Initialization:

The signer randomly chooses$k, r_1 \in Z_q^*$, compute $R = e(P,P)^k$ and $L = r_1 Q_{IDs}$ sends R, L to the user as a commitment.

Blinding:

The user randomly chooses $a, b \in Z_q^*$ as blinding factors, compute $R' = e\big(bQ_{IDs} + aP,\ P_{pub}\big)$, $V = h(H, R') + b$ where $H = H_2\big(ID_s,\ ID_v, m, R', e(d_{IDs}, r_1 Q_{IDv})\big)$and sends V to the signer.

Signing:

The signer sends back W, where $W = Vd_{IDs} + kP$.

Unblinding:

The user compute $W' = W + aP_{pub}$ and $V' = V - b$ outputs$< m, W', V' >$. Then$< W', V', L >$ is the blind signature of the message m.

Direct Verification:

Given purported signature $\sigma =< L, W', V' >$ on signerID_s , verifier ID_v and message m, ID_v verifies with his private key d_{IDv} as follows.

Compute $R' = e(W', P)e\big(Q_{IDs}, P_{pub}\big)^{-V'}$ and compute $H = H_2\big(ID_s, ID_v, m, R', e(d_{IDv}, L)\big)$

Accept the signature if and only if $V' = h(H, R')$.

Public Verification:

Given purported signature $\sigma =< L, W', V' >$ on signer ID_s , verifier ID_v and message m, to enable a third party T to verify it eitherID_s or ID_v computes $Aid = e(d_{IDv}, L) = e(d_{IDs}, r_2 Q_{IDv})$and send it to T along with R'. Compute $H = H_2(ID_s, ID_v, m, R', Aid)$. Accept if $V' = h(H, R')$.

Security analysis of the proposed scheme:

The following equations give the correctness of the proposed scheme.

$$h\Big(H, e(W', P)e\big(Q_{IDs}, P_{pub}\big)^{-V'}\Big)$$
$$= h\Big(H, e\big(W + aP_{pub}, P\big)e\big(Q_{IDs}, P_{pub}\big)^{-V'}\Big)$$
$$= h\Big(H, e(W, P)e\big(aP_{pub}, P\big)e\big(Q_{IDs}, P_{pub}\big)^{-V'}\Big)$$
$$= h\Big(H, e(Vd_{IDs}, P)e(kP, P)e\big(aP_{pub}, P\big)e\big(Q_{IDs}, P_{pub}\big)^{-V'}\Big)$$
$$= h\Big(H, e\big(Q_{IDs}, P_{pub}\big)^{V} e(kP, P)e\big(aP, P_{pub}\big)e\big(Q_{IDs}, P_{pub}\big)^{-V+b}\Big)$$
$$= h\big(H, e(P,P)^k e\big(aP + bQ_{IDs}, P_{pub}\big)\ \big)$$
$$= h(H, R') = V'$$

Security:

In the following, we will show that our ID-based Directed Blind Signature Scheme satisfies all the requirements stated in section-3.

Blindness Property:

To prove the blindness we show that given a valid signature $< m, W', V' >$ and any view $< R, V, W >$ there always exists a unique pair of blinding factors $a, b \in Z_q^*$. Since the blinding factors $a, b \in Z_q^*$ are chosen randomly, the blindness of the signature naturally satisfies. We can find more formal definition about the blindness.

Given a valid signature $< m, W', V' >$ and any view $< R, V, W >$ then the following equations must hold for $a, b \in Z_q^*$.

$$R' = e\big(bQ_{IDs} + aP,\quad P_{pub}\big).R \qquad (1)$$

$$V = h(H, R') + b \qquad (2)$$

$$W' = W + aP_{pub} \qquad (3)$$

$b = V - h(H, R')$ and $W' - W = aP_{pub}$.

It is obvious that $a, b \in Z_q^*$ is existed uniquely from (2) and (3). Next we show that such $a, b \in Z_q^*$ satisfies the first equation too. Obviously, due to the non-degenerate of the bilinear pairings we have $R' = e\big(bQ_{IDs} + aP,\ P_{pub}\big).R$
$\leftrightarrow e(R', P_{pub}) = e\big(e\big(bQ_{IDs} + aP,\ P_{pub}\big).R, P_{pub}\big)$.
So we only need to show that such a and b satisfy $e(R', P_{pub}) = e\big(e\big(bQ_{IDs} + aP,\ P_{pub}\big).R, P_{pub}\big)$.

We have $e\big(e\big(bQ_{IDs}+aP,\ P_{pub}\big).R,P_{pub}\big)$

$= e\big(e\big(bd_{IDs}+aP_{pub},\ P\big).R,P_{pub}\big)$

$= e\big(e(V-h(H,R')d_{IDs},P)e\big(aP_{pub},\ P\big).R,P_{pub}\big)$

$=e\big(e(V-h(H,R')d_{IDs},P)e(W'-W,\ P).R,P_{pub}\big)$

$= e\begin{pmatrix} e(Vd_{IDs},P)e(-h(H,R')d_{IDs},P)e(W',P) \\ e(W,P)^{-1}.R,P_{pub} \end{pmatrix}$

$= e\left(e(-h(H,R')d_{IDs},P)R'e\big(Q_{IDs},P_{pub}\big)^{V'},P_{pub}\right)$

$= e\begin{pmatrix} e\big(-h(H,R')Q_{IDs},P_{pub}\big) \\ R'e\big(h(H,R')Q_{IDs},P_{pub}\big),P_{pub} \end{pmatrix}$

$=e\big(R',P_{pub}\big).$

Thus the blinding factors always exist which lead to the same relation defined in the signature issuing protocol.

Unforgeability:

Assume that **A** is the adversary (he/she can be a user or any third party) holding the system parameters $params < G_1, G_2, e, P, P_{pub}, H_1, H_2, h >$ and the identity public key Q_{IDs} of the signer ID_s. A tries to forge a valid message-signature of the signer.

First, we assume that ***A*** performs the ID attack, i.e. ***A*** queries **Extract** qE (qE>0) times with (PARAMS, $ID_i \neq ID$) for i=1….qE. **Extract** returns to ***A*** the qE corresponding secret key d_{IDs_i}. We assume that qE is limited by a polynomial in k. If ***A*** can get a (ID_s', d_{IDs}'), such that$H_1(ID_s') = H_1(ID_s) = Q_{IDs}$, then he/she can forge a valid blind signature of the signer ID. But since H_1 is random oracle, **Extract** generates random numbers with uniform distributions. This means that ***A*** learns nothing from query results.

Next we assume that ***A*** had interacted with the signer ID, and let$< R, V, W >$be the view in the blind signature issuing phase. Since $W = Vd_{IDs} + kP$ and ***A*** knows W, V from W to get d_{IDs}, ***A*** must know k, but k is chosen randomly by signer. ***A*** Knows $R = e(P,P)^k$ but from r to get k, this is CDHP in G_1. We assume that CDHP in G_1 in intractable, so ***A*** cannot get the private information of the signer at the blind signature issuing phase. On the other hand, the signature and the verifying equation are same as Hess ID- based signature scheme. For any message m, if ***A*** can construct W' and V' such that $V' = h\left(H, e(W', P\,)e\big(Q_{IDs}, P_{pub}\big)^{-V'}\right)$, then ***A*** can forge a valid signature of Hess ID-based signature scheme (i.e., Hess ID-based signature scheme is proven to be secure against existential forgery on adaptive chosen message and ID attacks, under the hardness assumption of CDHP and the random oracle model) We claim that this attack is impossible.

Conclusion:

We proposed an ID-based Directed Blind Signature Scheme (ID-DBS) from bilinear pairings. This scheme allows a a user to obtain a signature on a message without revealing anything about the message to the signer; and sends it to the designated verifier. The designated verifier can only verify the validity of the signature and in case of trouble or if necessary he can prove the validity of the signature to any other party. This scheme is applicable when the message is sensitive to the receiver and also without revealing anything about the message to the signer. We proved that our ID-DBS scheme is secure against existential forgery under adaptive chosen-message attack and chosen-identity attack in the random oracle model. We have discussed the correctness and security analysis of the proposed scheme.

References:

1. D.Boneh and M.Franklin, “Identity-based encryption from the weil pairing”, In Proc.Of CRYPTO’01, LNCS 2139, pp.213-229, Springer-verlag, 2001.
2. P.S.L.M. Barreto, B. Libert, N. McCullagh and J. Quisquater, “Efficient and Provably Secure Identity-Based Signatures and Signcryption from Bilinear Maps”, In B.Roy, editor(s), Asiacrypt 2005, LNCS 3788, Springer-Verlag, 2005, pp. 515-532.
3. J.C.Cha and J.H.Cheon, “An identity-based signature from gap Diffie-Hellman groups”, Public Key Cryptography-PKC2003, LNCS 2567, Springer-Verlag, pp. 18-30, 2003.
4. D.Chaum. *Designated Confirmer Signatures*, Advances is Cryptology, EUROCRYPT– 94, LNCS Vol. 950, pages 86-91.
5. D.Chaum. *Zero- Knowledge undeniable signatures*, Advances in Cryptology, EUROCRYPT–90, LNCS, Vol. 473, pages 458-464, Springer- verlag,1991.
6. D. Chaum, “Blind signatures for untraceable payments”, In Proc. CRYPTO 82, pp.199-203, NY, 1983, Plenum.
7. L.C Guillou and J.J. Quisqter. *A Practical Zero – Knowledge Protocol fitted to security microprocessors minimizing both transmission and memory*, Advances in Cryptology, EUROCRYPT-88 LNCS, Vol. 330, pages 123-128, 1989.
8. F. Hess, “Efficient identity based signature schemes based on pairings”, SAC 2002, LNCS 2595, pp.310-324, Springer-Verlag, 2002.
9. S. Lal and M.Kumar. *A directed signature scheme and its Applications*, available at: http://arriv.org/abs/cs/0409035
10. R. Lee and Z. Cao. *A directed signature scheme based on RSA Assumption*, International Journal of Network Security, Vol. 2, No.3, pages 182-186, May 2006.
11. C.H.Lim and P.J. Lee. *Modified Maurer-yacobi scheme and its Applications.* Advances in Cryptology, AUSCRYPT-92, LNCS, Vol.718, pages 308 -323, Springer Verlag, 1992.
12. C.H. Lim and P.J. Lee. Directed signatures and application to threshold cryptosystems, *Security Protocols*, LNCS 1189, pages 131- 138, Springer-Verlag,1996.

13. T. Okamoto. *Designated confirmer signatures and public key Encryptions are equivalent*. Advances in Cryptology, CRYPTO–94, LNCS, Vol. 839, pages 61–74, Springer Verlag, 1994.
14. T.Okamoto, "Provable, Secure and Practical Identification Schemes and Corresponding signature schemes", In Advances in Cryptology-CRYPTO1984, Springer-Verlag,LNCS 740, pp.31-53,1992.
15. K.G.Paterson, "ID-based Signatures from Pairings on Elliptic Curves", IEEE Communications Letters, Vol.38, No.18, 2002, pp.1025-1026.
16. D.Pointcheval and J.Stern, "Provably Secure Blind signature Schemes", In Advances in Cryptology – ASIACRYPT 1992, Springer-Verlag, LNCS 1163, pp.252-26,1992.
17. D.Pointcheval and J.Stern, "New Blind Signature Signatures Equilent to Factorization", In proceedings of the 4th ACM Conference on Computer and Communications Security, pp.92-99, Zurich, Switzerland, 1997.
18. R.Rivest, A.Shamir, and L.Ad leman. *A method for obtaining digital signatures and public key cryptosystems*, communications of the ACM, Vol. 21, No. 2, pages 120-126, 1978.
19. C.P.Schnorr. *Efficient signature generation by smart cards*, Journal of Cryptology, Vol. 4(3), pages 161-174, Springer-verlag, 1994.
20. C.P. Schnorr, "Efficient Identification and Signatures for Smart cards", In G.Brassard(ed), In proceedings of CRYPTO 1989, Springer-Verlag,LNCS 435,pp.239-252,1990.
21. A,Shamir, "Identity-based cryptosystems and signature schemes", In Proc. Of CRYPTO'84, LNCS 196, pp. 47-53 Springer-verlag, 1984.
22. *B.Umaprasadarao, P.Vasudeva Reddy, T.Gowri, An efficient ID-based Directed Signature Scheme from Bilinear Pairings, eprint.iacr.org/2009/617.pdf.*
23. *B.Umaprasadarao, P.Vasudeva Reddy, "*ID-based Directed Serial Multisignature scheme from bilinear pairings", International Journal of Advanced Research in Computer Science, Vol. 1, No.4, pp.128-133,2010.
24. *P.Vasudeva Reddy, B. Umaprasada Rao, T.Gowri"* An ID-based Directed Proxy signatures schemes from bilinear pairings", Journal of Discrete Mathematical Science and Cryptography Vol. 13, No.5,pp.489-500,2010.