Volume 1, No. 4, Nov-Dec 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ID-based Directed Serial Multisignature Scheme from Bilinear Pairings

B.Umaprasada Rao
Department of Engineering Mathematics
College of Engineering, Andhra University
Visakhapatnam, India
buprasad@yahoo.co.in

Dr.P.Vasudeva Reddy*
Department of Engineering Mathematics
College of Engineering, Andhra University
Visakhapatnam, India
vasucrypto@yahoo.com

Abstract: Directed signature scheme allows only a designated verifier to check the validity of the signature issued to him; and at the time of trouble or if necessary, any third party can verify the signature with the help of the signer or the designated verifier as well. Due to its merits, directed signature scheme is widely used in situations where the receiver's privacy should be protected. A multisignature scheme is digital signature schemes in which multiple signers are jointly generate a valid signature for an identical message. Based on the nature of applications, the multisignatures have been categorized into two types: serial and parallel. In this paper, we propose an ID-based Directed Serial Multi Signature Scheme (ID-DSMS) from bilinear pairings by combining the concept of multisignatures and directed signatures. This scheme allows multiple signers to generate signatures on a message to a designated verifier such that the designated verifier can directly verify the validity of the signature issued to him. In case of necessary the designated verifier can prove the validity of the multisignature to any other party. We also prove that the proposed ID-DSMS scheme is secure against existential forgery under adaptive chosen-message attack and chosen-identity attack in the random oracle model by assuming that the CDH problem is hard.

Key Words: Multisignature, Directed signature, Bilinear Pairings, ID- based Cryptographic schemes.

I. INTRODUCTION

Digital signature is a cryptographic tool to authenticate electronic communications. A 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 most situations, the signer is generally a single person. However, in many cases the message is sent by one organization and requires the approval or consent of several people. In day-to-day life, many legal documents require signatures from more than one party, e.g., contracts, decision making process, petitions etc. In such cases, the signature generation is done by more than one consenting person.

To meet this requirement in the digital environment, cryptography provides a mechanism known as digital multisignature. Based on the nature of applications, multisigna tures have been categorized into two types: serial and parallel. In serial multisignature, a signer signs the message and sends it to the next signer for further processing; the next signer after verifying his predecessor's signature, signs the received component. The serial multisignature generation is considered to be complete when the last signer signs. Many financial transactions require serial multisignatures and verification at each level. For e.g., in the maker-checker-approval concept, where maker prepares the transaction and checker ensures the correctness of the transaction for approval. This process need to be followed in a sequence such that every signer is forced to verify his immediate predecessor's signature. In the case of parallel multisignature, the signature of each signer is carried out on the message itself but not on the signatures of the other signers. In order to complete the parallel multisignature generation, a designated clerk combines all the individual signatures after verifying them. Parallel multisignatures are useful in the organization where a flat reporting structure exists. Itakura and Nakammura [1] introduced the concept of multisignature. Since then, several schemes [2, 3, 4, 5, 6] for multisignatures have been proposed.

An efficient digital multisignature scheme [2] based on DLP has been proposed in 1994, in which the length and the verification time of the multisignatures are both fixed. For RSA [7] based schemes, there exists no efficient multisignature scheme in the literature due to the module clashing problem [8, 9]. But many of the above multisignature schemes are proposed under certificate based public-key cryptosystems. One may note that the traditional certificate authority (CA) based public-key cryptosystems require large amount of storage and computing time to manage certificate life cycle [10].

In 1985, Shamir [11] introduced the concept of identity (ID) based cryptosystem where a user's public-key could be easily derived from his identity and user's private key is generated by a trusted third party called PKG. ID-based cryptosystems are advantageous over the traditional PKCs, as key distribution and revocation are simplified [12]. ID-based PKC setting can be a good alternative for certificate based public key setting, especially when efficient key management and moderate security are redesigned. Several ID-based

encryption schemes and signature schemes [13, 14, 15, 16] have been proposed. But, no practical ID-based encryption had been known for a long time. Ever since Boneh and Franklin gave a practical ID-based encryption schemes from Weil pairing [17] in 2001, several ID-based signature scheme based on pairings were proposed [18, 19, 20, 21]. Due to the nice property of pairings, all these schemes signature schemes are simple and efficient.

However, there are so many situations, when the signed message is sensitive to the signature receiver. Signatures on medical records, tax information and most personal/business transactions are such situations. Signatures used in such situations are called directed signatures [22, 23, 24, 25, 26, 27, 28].

Consider the situations when the signed message requires approval or consent of several people and the signed message is sensitive to the signature receiver. To meet this requirement, it is necessary to combine the multisignatures with the concept of directed signatures. In this paper, we propose a digital signature scheme named as "An ID-based Directed Serial Multisignature from Bilinear Pairings". The ID-based Directed Parallel Multisignature from Bilinear Pairings was proposed in [29]. To the best of our knowledge our scheme is the first ID-based directed serial multisignature scheme using pairings. We use Hess's ID-based signature scheme [20] as the base for our scheme. The proposed scheme is secure against existence forgery under adaptive chosen message attack in the random oracle model assuming Computational Diffie-Helman Problem (CDHP) is hard.

The rest of the paper is organized as follows. In Section II, we describe background concepts on bilinear pairings and some related mathematical problems. In Section III, we present our ID-based Directed Serial Multisignature Scheme (ID-DSMS). Section IV gives security analysis of the proposed scheme. Finally, we conclude our work in section V.

II. PRELIMINARIES

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

A. 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:

[a] Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in G_1$ and all $a, b \in Z_q^*$

[b] Non–degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;

[c] Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

B. Computational problems

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

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 the following problems in G_1.

[a] 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.

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

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

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 a group can be found in super singular elliptic curves or hyper elliptic curves over finite fields, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [17, 20].

C. Hess-ID- based signature scheme

To prepare for our ID-DSMS scheme, we use the following ID-based signature scheme [20] given by Hess as the base.

[a] 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 2.1. He then selects $s \in_R Z_q^*$ randomly and computes the public key $P_{pub} = sP$, also picks a hash function $H_1: \{0,1\}^* \to G_1^*$ and another cryptographic hash function $h: \{0,1\}^* \times G_2 \to Z_q^*$. The PKG now publishes system parameters $params = <G_1, G_2, e, P, P_{pub}, H_1, h>$ and keeps $< s >$ secret as master key.

[b] 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.

[c] 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

$R = e(P_1, P)^k$,

$V = h(M, R)$,

$U = V d_{ID} + k P_1$.

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

[d] 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 $V = h(M, R)$.

III. PROPOSED SCHEME

In this section, we propose an ID-based Directed Serial Multisignature Scheme based on the Hess-ID-based signature scheme. In our ID-DSMS scheme, the set of n signers with identities $\{IDs_1, IDs_2, ..., IDs_n\}$ sequentially generates their individual signatures on the given message M and the final signer sends it to the designated verifier IDv. The designated verifier can directly verify the multisignature issued to him. In case of necessary, any third party can verify the validity of the multisignature. Our ID-DSMS scheme consists of the following five phases: System Setup, Key Extraction, Multisignature Generation, Direct Verification, and Public Verification.

A. System Setup

For a given security parameter l, the PKG chooses two groups G_1 and G_2 respectively be additive and multiplicative groups of prime order $q \geq 2^l$ with a bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$ and a generator $P \in G_1$, as described in 2.3.1. PKG then selects randomly $s \in_R Z_q^*$ and computes the public key $P_{pub} = sP$, also picks cryptographic hash functions $H_1, H_2: \{0,1\}^* \rightarrow G_1^*$ and $h: \{0,1\}^* \times G_2 \rightarrow Z_q^*$. The PKG now publishes system parameters as $params = <G_1, G_2, e, P, P_{pub}, H_1, H_2, h>$ and keeps secret $< s >$ as master key.

B. Key Extraction

Let I=$\{IDs_1, IDs_2, ..., IDs_n\}$ be the set of *n* signers. Each signer in I sends his identity IDs_i to PKG to get his private key $d_{IDs_i} = sQ_{IDs_i}$, where $Q_{IDs_i} = H_1(IDs_i)$.

The key extraction phase requires secure channel for the PKG to deliver the private key of signers. This can be overcome efficiently by the secure key issuing protocol proposed in [30].

C. Multisignature Generation

In this phase, a signer signs the message M and sends it to the next signer for further processing; the next signer after verifying his predecessor's signature, signs the received component. The multi signature generation process to be complete when the last signer IDs_n signs the received component from IDs_{n-1}. Thus *n* signers with identities $\{IDs_1, IDs_2, ..., IDs_n\}$ sequentially generate the multisignature and the last signer IDs_n sends it to the designated verifier IDv. To have a Multisignature on message M, without loss of generality, we present it is the following stages.

[a] Signature Generation by First Signer To sign a message M, the first signer

IDs_1 Picks two random integers

$k_1, r_1 \in Z_q^*$ And computes

$U_1' = e(P, P)^{k_1}$, $L_1 = e(d_{IDs_1}, r_1 Q_{IDs_2})$,

$R_1 = r_1 Q_{IDs_1}$. Set $U_1 = U_1'$.

Also he computes $V_1 = h(t_1, U_1)$,

Where $t_1 = H_2(M, L_1)$, and then

$W_1 = V_1 d_{IDs_1} + k_1 P$.

The signature by the first signer is the tuple (W_1, V_1, R_1) which he sends to the second signer IDs_2 along with the message M.

[b] Verification and Signature by Immediate (i^{th}) Signer

The i^{th} signer verifies the signature $(W_{i-1}, V_1, V_2, ..., V_{i-1}, R_{i-1})$ Received from $(i-1)^{th}$ Signer by computing

$U_{i-1} = e(W_{i-1}, P) e\left(\sum_{j=1}^{i-1} V_j Q_{IDs_j}, -P_{pub}\right)$ And

$t_{i-1} = H_2\left(M, e\left(d_{IDs_i}, R_{i-1}\right)\right)$.

The signature is accepted if and only

If $V_{i-1} = h(t_{i-1}, U_{i-1})$.

For generating his signature, the i^{th} signer IDs_i picks two random integers

$k_i, r_i \in Z_q^*$ And computes

$U_i' = e(P, P)^{k_i}$,

$L_i = e(d_{IDs_i}, r_i Q_{IDs_{i+1}})$, $R_i = r_i Q_{IDs_i}$.

Set $U_i = U_i' U_{i-1}$. Also he computes

$V_i = h(t_i, U_i)$, where

$t_i = H_2(M, L_i)$, and

Then $W_i = W_{i-1} + V_i d_{IDs_i} + k_i P$.

He then sends the partial multisignature $(W_i, V_1, V_2, ..., V_i, R_i)$ to the $(i+1)^{th}$ signer.

We may note that i^{th} signer can't generate his signature without verifying the signature of $(i-1)^{th}$ signer, as it requires the extraction of U_{i-1} from the predecessor's signature $(W_{i-1}, V_1, V_2, ..., V_{i-1}, R_{i-1})$.

This ensures the forced verification.

[c] Verification and signature by final (n^{th}) signer

The n^{th} signer IDs_n verifies the signature $(W_{n-1}, V_1, V_2, ..., V_{n-1}, R_{n-1})$ Received From $(n-1)^{th}$ signer by computing

$$U_{n-1} = e(W_{n-1}, P)\, e\left(\sum_{j=1}^{n-1} V_j Q_{IDs_j}, -P_{pub}\right)$$

and $t_{n-1} = H_2\left(M, e\left(d_{IDs_n}, R_{n-1}\right)\right)$.

The signature is accepted if and only if $V_{n-1} = h(t_{n-1}, U_{n-1})$]

The last signer (n^{th} signer) IDs_n generates his signature to a designated verifier IDv. For this IDs_n selects two random integers $k_n, r_n \in Z_q^*$ and computes

$U_n^{'} = e(P, P)^{k_n}$,

$L_n = e\left(d_{IDs_n}, r_n Q_{IDv}\right)$,

$R_n = r_n Q_{IDs_n}$.

Set $U_n = U_n^{'} U_{n-1}$.

Also he computes $V_n = h(t_n, U_n)$,

where $t_n = H_2(M, L_n)$, and

$W_n = W_{n-1} + V_n d_{IDs_n} + k_n P$.

He then sends the final multisignature $\sigma = (W_n, V_1, V_2, ..., V_n, R_n)$ along with the message M to the designated verifier ID_V.

D. Multisignature Direct Verification

On receiving a multisignature $\sigma = (W_n, V_1, V_2, ..., V_n, R_n)$ along with the message M, the designated verifier ID_V verifies validity of the signature. For this ID_V computes $U_n = e(W_n, P)\, e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right)$ and $t_n = H_2\left(M, e\left(d_{IDv}, R_n\right)\right)$.

The designated verifier ID_V accepts the signature if and only if $V_n = h(t_n, U_n)$.

E. Multisignature Public Verification

Given a multisignature $\sigma = (W_n, V_1, V_2, ..., V_n, R_n)$, signers $IDs_1, IDs_2, ..., IDs_n$, designated verifier ID_V and message M, to enable a third party T to verify it, either the last signer IDs_n or the designated receiver ID_V provides an $Aid = L_n = e\left(d_{ID_v}, R_n\right)$.

Then T computes $U_n = e(W_n, P)\, e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right)$ and $t_n = H_2(M, Aid)$.

T accepts the signature if and only if $V_n = h(t_n, U_n)$.

IV. ANALYSIS OF THE PROPOSED SCHEME

In this section, first we show that the correctness of the scheme and then we discuss security analysis of our ID-DSMS.

A. Proof of correctness

The following equations give the correctness of the scheme.

$$e(W_n, P)\, e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right)$$

$$= e\left(\sum_{j=1}^{n} V_j d_{IDs_j} + k_j P, P\right) e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right)$$

$$= e\left(\sum_{j=1}^{n} V_j d_{IDs_j}, P\right) e\left(\sum_{j=1}^{n} k_j P, P\right) e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right)$$

$$= e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, P_{pub}\right) e\left(\sum_{j=1}^{n} k_j P, P\right) e\left(\sum_{j=1}^{n} V_j Q_{IDs_j}, -P_{pub}\right) =$$

$$e\left(\sum_{j=1}^{n} k_j P, P\right) = \prod_{j=1}^{n} e(P, P)^{k_j} = \prod_{j=1}^{n} U_j^{'} = U_n$$

B. Security Analysis for our ID-DSMS

In this section, we will analyze the security of our ID-DSMS scheme from existential forgery under adaptive chosen-message attack. Informally, an existential forgery in ID-DSMS scheme refers to that the adversary attempts to forge an ID-DSMS of messages and identities of signers at its choice. In 2004, Bellare et al. [31] proved that the basic identity based signature scheme (Hess) [20] is secure against existential forgery under adaptive chosen-message attack and adaptive chosen-identity attack in the random oracle model. The two hash functions H_1 and H_2 which are used in our

proposed scheme will be treated as random oracles in the following security analysis.

Theorem 1: The proposed ID-DSMS scheme is secure against existential forgery under adaptive chosen-message attack and chosen-identity attack in the random oracle model.

Proof: Let $A_{ID-DSMS}$ and A_{IBS} be polynomial-time adversaries of our proposed ID-DSMS scheme and the basic IBS (Hess) scheme, respectively. We can prove this theorem according to [31]. The main idea is that if the adversary $A_{ID-DSMS}$ can forge a valid multisignature on an arbitrary message M without interacting with the honest signer, then the adversary A_{IBS} can also forge a valid basic signature on message M of an honest message signer.

We now describe the detailed proof as follows. The adversary A_{IBS} chooses an identity ID and requests the hash oracle and signing oracle of any message. A_{IBS} will run $A_{ID-DSMS}$ to simulate a single honest signer. When $A_{ID-DSMS}$ wants to get a valid directed multisignture, it runs of sign oracle for A_{IBS}, A_{IBS} simulates $A_{ID-DSMS}$'s random hash oracle using its own oracle. A_{IBS} will then request the signing oracle with the identity of honest signer ID and the corresponding message. The signing oracle will generate the output to $A_{ID-DSMS}$. It is easy to know that the output of $A_{ID-DSMS}$ is a valid directed multisignture (a successful forgery for message) as long as the answer from A_{IBS} is a valid signature. However, according to [31], no valid basic identity-based signature can be generated from A_{IBS}. Therefore, our proposed ID-DSMS scheme is secure in the random oracle model.

***Theorem* 2**: The proposed ID-DSMS is really a directed signature.

Proof: To verify a multi signature σ, an $Aid = L_n = e\left(d_{ID_v}, R_n\right)$ must be available. Therefore, only the designated verifier can verify its authenticity due to his private key d_{ID_V}. As far as a third party T is concerned, to compute *Aid* is equivalent to solve the CDH problem. However, when third party T holds *Aid* with the help of the last signer or the designated verifier, he can easily verify the multisignature. Hence our proposed ID-DSMS scheme is actually a directed signature scheme.

V. CONCLUSION

We proposed an ID-based Directed Serial Multi Signature Scheme (ID-DSMS) from bilinear pairings by combining the concepts of multisignatures with directed signatures in the ID-based setting. This scheme allows multiple signers to generate multisignature to a designated verifier. The designated verifier can directly verify the validity of the multisignaute and he can prove the validity of multisignature to any third party whenever necessary. Our scheme requires a forced verification at each level, avoiding the overlooking in verifying the signature of the predecessor. Also our scheme is efficient in the sense that the verification time of multi signature is same as the verification time of a single signature. This scheme is applicable when the message requires approval of several people and the signed message is sensitive to the receiver. We have proved that the proposed ID-DSMS scheme is secure against existential forgery under adaptive chosen-message attack and chosen-identity attack in the random oracle model with the assumption that the CDH problem is intractable.

VI. REFERENCES

[1] Itakurak and Nakamura, "A public-key cryptosystem suitable for Digital Multisignatures", NEC Research and Develop, 1983, pp. 1-8.

[2] T .Okamoto, "A digital Multi-signature scheme using bijective PKC", ACM Transactions on Computer Systems, Vol 6, No - 8, 1988, pp. 432-441.

[3] L.Harn and T.Kiesler, "New Scheme for Digital multisignatures", Electronic Letters 25(15), 1989, pp.1002-1003.

[4] T.Hardjono and Y.Zheng, "A practical Digital Multisigna ture Scheme Based on DLP", Advance in cryptology – AUSCRYPT-92, 1991, pp. 16 – 21.

[5] L. Harn, "Group oriented (t, n) threshold digital signature scheme and digital multisignature", IEEE Proc. of Comput.Digit.Tech.141 (5), 1994, pp.307-313.

[6] K.Ohta and T.Okamoto, "A digital multisignature scheme based on Fiat-Shamir scheme", Advance in Cryptology ASIACRYPT-91, 1991, pp. 75-79.

[7] R.Rivest, A. Shamir and L.Adleman, "A method for obtaining digital signatures and public key cryptosys tems", Commun. Assoc. Comp. Mach. 21(2), 1978, pp.120-126.

[8] S-F.Pon, E-H.Lu and J-Y.Lee, "Dynamic reblocking rsa-based multisignatures scheme for computer and communication", IEEE Commun. Lett.6 (1), 2001, pp.432-44.

[9] T.Kiesler and L.Harm, "RSA blocking and multisignature schemes with no bit expansions", Elecronics Letters 26(18), 1990 , pp.1490-1495.

[10] P.Guttman, "PKI: It's not dead, Just resting", IEEE Computer, 35(8), pp. 45-49.

[11] A.Shamir, "Identity-based cryptosystem and signature scahemes", In: Blakley, G.R., Chaum,D.(eds.), Advances in Cryptology, Proceedings of CRYPTO'84, LNCS 196, Springer, Berlin, 1985, pp.47-53.

[12] M.C.Gorantla, R.Gangishetti and A.Saxena, "A survey on ID-based cryptographic primitives", In IACR Crypology ePrint Archive. Report 2005/094.

[13] H. Tanaka, "A realization scheme for the identity-based cryptosystem", Advance in CRYPTO'87, LNCS 293, Springer-Verlag, , 1987, pp.341-349

[14] S. Tsuj and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem", IEEE Journal of Selected Areas in Communications, Vol.7, No.4, 1989, pp.467-473.

[15] U.Maurer and Y.Yacobi, " Noninteractive public-key cryptography", Advance in Cryptology, EUROCRYPTO'91, LNCS 547, Springer-Verlag, 1992, pp.498-50.

[16] A.Fiat and A.Shamir, "How to prove yourself: Practcal solutions to identification and signature problems", Advance in CRYPTO'86, LNCS263, Springer-Verlag, , 1987, pp.77-94.

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

[18] X.Yi, "An identity-based signature scheme from the Weil-pairing", IEEE Communication Letters, 7(2), 2003, pp.76-78.

[19] J.C.Cha and J.H.Cheon, "An identity-based signature from gap Diffie-Hellman groups", Public Key Cryptography-PKC2003, LNCS 2567, Springer-Verlag, 2003, pp. 18-30.

[20] F. Hess, "Efficient identity based signature schemes based on pairings", Selected Areas in Cryptography, SAC 2002, Springer-Verlag, 2003, 2002, pp.310-324.

[21] A. Boldyreva, "Threshold signatures, Multisignatures, and blind signatures based on GDH group signature scheme", In proceedings of PKC, LNCS 2567, Springer-Verlag, Berlin, 2003, pp.31-46.

[22] D.Chaum, "Designated confirmer signatures", Advances in Cryptology – EUROCRYPT'94, LNCS 950, Springer-Verlag, 1994, pp. 86–91.

[23] R.Lu and Z.Cao, "A directed signature scheme based on RSA assumption", International Journal of Network Security 2 (3), 2006, pp182– 186.

[24] C.H.Lim and P.J.Lee, "Modified Maurer–Yacobi's scheme and its applications", Advances in Cryptology, AUSCRYPT'92, LNCS 718, Springer-Verlag, 1992, pp.308–323.

[25] 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.

[26] J. Sun, G. Li Chem and Yang, "Identity based directed signature scheme from bilinear pairings", In IACR Cryptology e-Print Archive, Report 2008/305. http://eprint.iacr.org/2008/305.pdf.

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

[28] B.Umaprasada Rao, P.Vasudeva Reddy and T.Gowri., "An efficient ID-based Directed Signature Scheme from Bilinear Pairings", Cryptology e-print Archive Report 2009/617. http://eprint.iacr.org/2009/617.pdf.

[29] B.Umaprasada Rao, P.Vasudeva Reddy and T.Gowri., "ID-based Directed Multisignature Scheme from Bilinear Pairings", In the Proceedings of National conference on Advanced Pattern Mining and Multimedia Computing(APMMC2010), NIT- Trichy, pp.294-298.

[30] R.Gangishetty, M.C.Gorantla, M. L. Das, A. Saxena, and V.P.Gulati, "An efficient secure key issuing protocol in ID-based Cryptosystem", In proceedings of the International Conference on IT : Coding and computing (ITCC2005), Vol.1, IEEE Computer society, 2005, pp. 674-678.

[31] M.Bellare, C. Namprempre, G. Neven, "Security proofs for ID-based identification and signature schemes", Advances in Cryptology, EUROCRYPT 04, LNCS 3023, Springer-verlag, Berlin,2004, pp.268-28.