ID-based Directed Threshold Multisignature Scheme from Bilinear Pairings

[1]P. Vasudeva Reddy, (vasucrypto@yahoo.com)
[1]B. Umaprasada Rao, (buprasad@yahoo.co.in)
[2]T. Gowri (gowri3478@yahoo.com)

1. *Department of Engineering Mathematics, Andhra University, Visakhapatnam, A.P, India.*
2. *Department of Electronics and communication Engineering, ASCET, Gudur, A.P, India.*

Abstract - Multi signature is a signature scheme in which signers jointly generate a signature on a message. Threshold multisignature combines the traits of threshold signature and multisignature. In threshold multisignature, a group of users jointly generate a valid multisignature on a message and any one can verify the validity of the multisignature. However, in some applications the signed message is sensitive to the signature receiver. 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. By combining all these ideas, in this paper, we propose an ID-based Directed Threshold Multisignature Scheme from bilinear pairings. To the best of our knowledge this is the first directed threshold mulitsignature scheme in the ID-based setting from bilinear pairings. The security of the proposed scheme is based on the Computational Difie-Hellman Problem. Also we have discussed the security properties of the proposed scheme namely, robustness and unforgeability.

I. 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 most situations, the signer is generally a single person. However, in some cases the message is sent by one organization and requires the approval or consent of several people. In these cases, the signature generation is done by more than one consenting person. A common example of this policy is a large bank transaction, by one organization, which requires the signature of more than one partner. Such a policy could be implemented by having a separate digital signature for every required signer, but this solution increases the effort to verify the message linearly with the number of signer. To solve these problems, Multisignature schemes [10, 19, 12, 18] and threshold signature schemes [7, 8, 9, 11] are used where more than one signers share the responsibility of signing messages. Threshold signature was introduced by Desmedt and Frankle [8]. In this paradigm, if *t* or more users collude, they can impersonate any other set of users to generate signatures. This case implies that a malicious subgroup of users can generate signatures without taking any responsibility. To solve this problem, the method of threshold multisignatue is presented [15], which combines idea of threshold signature with the idea of multisignature. It can prevent a group of malicious users from impersonating other users through the generation of signatures.

In 1984, Shamir introduced the concept of identity based (ID-based) systems to simplify key management procedures of CA-based Public Key Infrastructure (PKI) [22]. Since then, several ID-based signature schemes have been proposed [21, 20, 13, 5, 3,2]. ID-based systems can be a good alternative for CA-based systems from the viewpoint of efficiency and convenience. ID-based systems have a property that a user's public key can be easily calculated from his identity by a publicly available function, while his private key can be calculated by a trusted Key Generation Center (KGC). They enable any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted KGC issues a private key to each user when he first joins the network.

Recently, several threshold signature schemes from bilinear parings have been proposed. Boldyreva proposed a robust proactive threshold signature scheme which works any Gap Diffie-Hellman(GDH) group [3]. Baek and Zheng formalized the concept of identity based threshold signature and gave the first provably secure scheme [1]. Cheng et al. proposed an ID-based signature from m-torsion groups of super singular elliptic curves [6]. In these schemes, if *t* or more users collude, they can impersonate any other set of users to generate signatures, which is similar to regular threshold schemes.

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 [4, 23, 24, 16 ,17]. In directed signature scheme, the signature receiver has full control over the signature verification process and can prove the validity of the signature to any third party, whenever necessary. Nobody can check the validity of signature without his cooperation.

In this paper, by combining all these ideas, we propose a digital signature scheme named as "An ID-based Directed Threshold Multisignature from Bilinear Pairings". To the best of our knowledge there is no existing identity based directed threshold multisignature scheme using pairings. We use Hess's ID-based signature scheme [13] 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-Hellman Problem (CDHP) is hard. The rest of the paper is organized as follows. In Section 2, we describe background concepts on bilinear pairings and some related mathematical problems. In Section 3, we present our proposed ID-based Directed Threshold Multisignature Scheme (ID-DTMS). Section 4, gives security analysis of the proposed scheme. Finally, we conclude our work in section 5.

II. PRELIMINARIES

In this section, we will briefly review the basic concepts of bilinear pairings and some related mathematical problems, and then we introduce ID-based public key setting from bilinear pairings. Finally, we will introduce Baek and Zheng's computationally verifiable secret sharing scheme based on bilinear pairing (CVSSBP) [1].

2.1 Bilinear Pairings

Let G_1 be an 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 $a, b \in Z_q^*$.

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 $P, Q \in G_1$.

Now we describe some mathematical problems in G_1.

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 CDHP and DLP are intractable. When the DDHP is easy but the CDHP is hard on the group G. we call G as a Gap-Diffie-Hellman (GDH) group.

2.2 ID based Public-Key setting using pairings

ID-based public key setting involves a Key Generation Centre KGC and a group of users. The basic operations consist of Setup and Private Key Extraction (simply Extract). When we use bilinear pairings to construct ID-based Public Key Cryptography (IDPKC), Setup and Extract can be implemented as follows:

Let P be a generator of G_1. Remember that G_1 is an additive group of prime order q and the bilinear pairing is given by $e: G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H_1: \{0,1\}^* \to G_1^*$ *and* $H_2: \{0,1\}^* \to Z_q^*$.

Setup: KGC chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. KGC publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and

keeps s as the master key, which is known only by it self.

Extract: A user submits his identity information ID to KGC. KGC computes the user's public key as $Q_{ID} = H_1(ID)$, and returns $d_{ID} = sQ_{ID}$ to the user as his private key.

2.3 CVSSBP Scheme

Baek and Zheng proposed a computationally secure verifiable secret sharing scheme based on bilinear pairing (CVSSBP)[1]. This scheme will be used to distribute a private key associated with an identity into a number of signature generation servers.

Let $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$ be a set of parameters, as defined in section 2.2. Suppose that a threshold t and the number of servers n satisfies $1 \le t \le n$. To share a secret $S \in G_1$ among n parties, a dealer performs the following steps.

1. Chooses $F_1, F_2, ...F_{t-1}$ uniformly at random from G_1^* and construct a polynomial-like function (PLF) $F(x) = S + xF_1 + ... + x^{t-1}F_{t-1}$ for $x \in Z_q$ and computes $S_i = F(i)$ and verification key $Y_i = e(S_i, P)$ for $i = 0, ...n$. Note that $S_0 = S$.

2. Sends S_i to user A_i secretly while making Y_i public for $i = 1, ...n$. Broadcasts $\alpha_0 = e(S, P)$ and $\alpha_j = e(F_J, P)$ for $j = 1, ...t-1$.

3. Each user A_i then checks whether its share S_i is valid by computing $e(S_i, P) = \prod_{j=0}^{t-1} \alpha_j^{i^j}$.

III. PROPOSED SCHEME (ID-DTMS)

(ID-based Directed Threshold Multi signature Scheme)

Suppose a system involves a trusted KGC, a designated combiner DC and a group of users $A_1, A_2, ...A_n$. KGC is incharge of setting system parameters $parms = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, and computing all user's private keys. Let ID_i be the identity of the user A_i. Let B be any user subset of size $t(|B| = t)$. For any $i \in B$, we can define Lagrange's interpolation coefficients $\lambda_{0,i}^B = \prod_{j \in B, j \ne i} \frac{0-j}{i-j}$. Our ID-based scheme is described as follows:

Phase-I: Initialization.

KGC selects a random integer $s \in Z_q^*$ and sets $P_{pub} = sP$. KGC computes public key of A_j as $Q_{IDs}^{(j)} = H_1(ID_j)$ and returns $d_{IDs}^{(j)} = sQ_{IDs}^{(j)}$ to the user as his private key. Without loss of generality, let ID_o is a trusted dealer TD, which distributes his private key d_{IDs_o} to n users. TD $(i.e. ID_0)$ runs CVSSBP to distribute d_{IDs_o} to n users. Each user A_j gets private share $d_{IDs}^{(0,j)}$ from TD, simultaneously A_j gets his private key d_{IDs}^{j} from KGC. $d_{IDs}^{(0,j)}$ and $Y_j = e\left(d_{IDs}^{(0,j)}, P\right) \in G_2$ are private share and public/verifiable information, we have : $\prod_{i \in B} Y_i^{\lambda_{0,i}^B} = e\left(H_1(ID_0), P_{pub}\right)$.

Phase2: Partial Signature Generation

Let M be the message to be signed. To generate the partial signature on M, each signer A_j performs the following steps:

Step1: Chooses a random integer $k_j, r_j \in Z_q^*$ and computes $U_j = e(P_1, P)^{K_j}, R_j = r_j Q_{IDs}^{(j)}$ and $L_j = e\left(d_{IDs}^{(j)}, r_j Q_{IDv}\right)$ and broadcast U_j, L_j, R_j to the remaining $(t-1)$ signers and DC.

Step2: Computes U, L and R after receiving all U_j, L_j, R_j from $A_j \in B$ as $U = \prod_{j \in B} U_j, L = \prod_{j \in B} L_j$ and $R = \sum_{j \in B} R_j$.

Step3: Also computes $V_j = h(H, U_j), V = h(H, U)$, where $H = H_2(M, L)$. And then computes as $W_j = V\left(\lambda_{0,j}^B . d_{IDs}^{(0,j)} + d_{IDs}^{j}\right) + K_j P_1$.

The partial signature on message M is $\sigma_j = \left(W_j, V_j\right)$.

Step4: Sends $\sigma_j = \left(W_j, V_j\right)$ to DC as his partial signature on message M.

Phase3: Partial Signature Verification

DC verifies that each individual signature by checking the equality.

$$V_j = h\left(H, U_j\right), \text{where } \mathrm{U_j} = e\left(W_j, P\right)\left[e\left(Q_{IDs}^{j}, P_{pub}\right)\left(Y_j^{\lambda_{0,j}^{B}}\right)\right]^{-V}$$

.

Phase4: Threshold Multisignature Generation

If all the partial signatures are valid, DC combines them to W, $W = \sum W_j$.

Thus $\sigma = (W, V, R)$ is a threshold multisignature of message M.

Phase 5: Direct Verification

On receiving the threshold multisignature $\sigma = (W, V, R)$ on message M, the designated verifier computes

$U = e\left(W, P\right) e\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}$ and

$H = H_2\left(M, e\left(d_{ID_V}, R\right)\right)$.

Accepts the threshold multisignature if and only if $V = h\left(H, U\right)$.

Phase6: Public Verification

Given a threshold multisignature $\sigma = \left(W, V, R\right)$ on signers identities $ID_1, ID_2, ...ID_n$, verifier ID_V and message M, to enable a third party T to verify it, either DC (on behalf of signers) or ID_V computes Aid $= e\left(d_{ID_V}, R\right) = L$ and sends it to T. Then T computes $H = H_2(M, Aid)$ and

$$U = e\left(W, P\right) e(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}.$$

Accepts the threshold multisignature if and only if $V = h(H, U)$.

Correctness of the threshold multisignature

$$e(W,P)\, e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\sum W_j, P\right) e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\sum V\left(\lambda_{0,j}^{B} . d_{IDs}^{(0,j)} + d_{IDs}^{j}\right) + K_j P_1, P\right) e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\sum V\left(\lambda_{0,j}^{B} . d_{IDs}^{(0,j)} + d_{IDs}^{j}\right), P\right) e\left(\sum K_j P_1, P\right) e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\sum \lambda_{0,j}^{B} . d_{IDs}^{(0,j)}, P\right)^{V} e\left(\sum d_{IDs}^{j}, P\right)^{V} e\left(\sum K_j P_1, P\right) e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= \prod e(d_{IDs}^{(0,j)}, P)^{\lambda_{0,j}^{B} V} . e\left(\sum Q_{IDs}^{j}, P_{pub}\right)^{V} e\left(\sum K_j P_1, P\right) e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\mathrm{H_1}\left(ID_0\right), P_{pub}\right)^{V} . e\left(\sum Q_{IDs}^{j}, P_{pub}\right)^{V} \prod e(K_j P_1, P) . e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right)$$

$$= e\left(\sum \mathrm{Q_{IDs}^{j}} + H_1(ID_0), P_{pub}\right)^{V} e\left(\left(\sum Q_{IDs}^{j} + H_1(ID_0)\right), -P_{pub})^{V}\right) \prod e(P_1, P)^{K_j}$$

$$= \mathrm{U}.$$

IV. Security Analysis of the Proposed ID-DTMS.

To analyze the security, the properties of robustness and unforgeability of the scheme should be considered.

1) **Unforgeability**: An adversary chooses the players he wants to corrupt in advance. Here corruption means that the adversary can manage to know the private key of the corrupted players. Unforgeability means that an adversary, even if having corrupted up to $t-1$ players of the group, cannot produce a valid pair $\left(M, \sigma\right)$, where M is a message having never been signed by the signers.

2) **Robustness**: An adversary having corrupted up to $t-1$ players, or $t-1$ co-operated malicious players of the group cannot prevent it from generating a valid signature,

Definition 1: A threshold multisignature scheme is called secure if it has the properties of unforgeability and robustness.

Theorem 1: The proposed ID-DTMS has the property of robustness.

Proof: The threshold multisignature is reconstructed from at least t partial signatures. The Designated Combiner (DC) first verifies all the partial signatures and then chooses the valid ones to reconstruct a threshold signature. Even if having corrupted up to $(t-1)$ signers, since there is no way to get the t^{th} valid partial signature, the adversary still cannot produce a valid threshold signature. While DC can get t valid partial signatures, thus can produce a valid threshold multisignature.

Theorem 2: The proposed ID-DTMS has the property of unforgeability.

To prove the property of unforgeability of the proposed ID-DTM scheme, we use the method given by R.Gennaro et al. [9], which indicates that a threshold multisignature is unforgeable if the underlying signature is secure and the threshold multisignature is simulatable.

A threshold signature scheme is simulatable if the following properties hold:

1) The private key generation and distribution protocol is simulatable. That is, there is a simulator to simulate the view of the adversary on the execution.

2) The threshold multisignature generation protocol as simulatable. That is, there exists a simulator to simulate the view of the adversary on the execution of threshold multisignature generation.

The private key generation and distribution protocol in our scheme is a variant of the well-known Baek and Zheng's computationally secure verifiable secret sharing scheme (CVSSBP)[1]. As discussed in [25], we can easily prove that our threshold multisignature generation protocol is simulatable. So, our ID-DTMS is simulatable. Also, the underling signature scheme [13], for the proposed scheme, is secure against existentially forgery under adaptive chosen message attack and given ID attack in the random oracle model by assuming Computational Diffie- Hellman Problem (CDHP) is hard. Therefore, the proposed ID-DTMS is unforgeable.

Theorem 3: The proposed ID-DTMS is really a directed signature.

Proof: To verify a threshold multisignature $\sigma = (W, V, R)$, $Aid = e(d_{IDv}, R) = L$ must be available . Therefore, only the designated verifier can verify its authenticity due to his private key d_{IDv}. As far as a third party is concerned, to compute *Aid* is equivalent to solve the CDHP. However, when a third party holds *Aid* with the help of DC (on behalf of the signers) or a designated verifier, he can easily verify the multisignature. Hence the proposed ID-DTMS scheme is actually a directed signature scheme.

Conclusions

We proposed an ID-based Directed threshold Multisignature Scheme (ID-DTMS)from bilinear pairings. This scheme is applicable when the signed message is sensitive to the signature receiver; and signatures are generated by the cooperation of a number of people from a given group of senders. In this scheme, any malicious set of signers cannot impersonate any other set of signers to forge the signatures. The proposed ID-DTMS scheme is robust and is unforgeable in the random oracle modal by assuming the CDH problem is hard.

References

[1] J.Baek and Y.L.Zheng, "Identity-Based Threshold Signature Scheme from the Bilinear Pairings", TCC'04, IEEE Computer Society, , 2004, pp.124-128.

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

[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, 2003, pp.18-30.

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

[5] X.F.Chen, F.G.Zhang and K.Kim, "A New ID-based Group Signature Scheme from Bilinear Pairings", In Proceedings of WISA'03, LNCS 2908, Springer-Verlag, 2003, pp.585-592.

[6] X.G.Cheng, J.M.Liu and X.M.Wang, "An Identity-Based Signature and Its Threshold Version", Advanced Information Networking and Applications-AINA'05, IEEE, 2005, pp. 973-977.

[7] Y.Desmedt, "Threshold cryptography", European Transactions on Telecommunications and Related Technologies. Vol. 5, No. 4, 1994, pp.35 – 43.

[8] Y.Desmedt and Y.Frankel, "Shared Generation of Authenticators and Signatures", Advances in Cryptology-Crypto'91, LNCS 576, Springer-Verlag, 1992, pp.457-469.

[9] R.Gennaro, S.Jarecki, H.Krawczyk and T.Rabin, "Robust threshold DSS signature", Advances in EuroCrypto'96,LNCS 1070, Springer–Verlag, 1996, pp.354 – 371.

[10] T.Hardjono and Y.Zheng, "A practical Digital Multisignature Scheme Based on DLP", Advance in cryptology –Auscrypt-92, 1991, pp. 16 – 21.

[11] L.Harn, "(t, n) Threshold signature scheme and digital multisignature", Workshop on cryptography and Data security, Proceedings, Chung Cheng Institute of Technology, ROC,June 7-9,1993, pp.61-73.

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

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

[14] W.B.Lee and C.C.Chang, "(*t, n*) Threshold Digital Signature with Traceability Property", Journal of Information Science and Engineering, Vol.15, No.5, 1999, pp. 669-678.

[15] C.Li, T.Hwang, and N.Lee, "Threshold-Multisignature Schemes where Suspected Forgery Implies Traceability of Adversarial Shareholders", Advances in Cryptology-Eurocrypt'94, LNCS 950, Springer-Verlag, 1995, pp. 194-204.

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

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

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

[19] T.Okamoto, “A digital Multi-signature scheme using bijective PKC”, ACM transactions on computer systems, Vol.6, No.8, 1988, pp. 432-441.

[20] K.G.Paterson, “ID-based Signatures from Pairings on Elliptic Curves”, IEEE Communications Letters, Vol.38, No.18, 2002, pp.1025-1026.

[21] R.Sakai, K.Ohgishi and M.Kasahara, “Cryptosystems Based on Pairing”, The 2000 Symposium on Cryptography and Information Security-SCIS'00, Okinawa, Japan, 2000, pp.26-28.

[22] A.Shamir, ”Identity-based cryptosystem and signature scahemes”, In: Blakley.G.R, Chaum.D (eds.) Advances in cryptology Proceedings of Crypto’84, Lecture Notes in Computer Science, vol.196, 1985, pp47-53, Springer, Berlin.

[23] Sun, J.Li, G.Chem, Yang, “Identity based directed signature scheme from bilinear pairings”, In IACR Crypology ePrint Archive. Report 2008/305.

[24] Sunderlal and Manoj Kumar, “ A directed signature scheme and its applications“, Proceedings of National conference on Information Security, Newyork, 8-9 Jan 2003, pp. 124-132.

[25] C. Xiangguo, L.Jingmei., W.Xinmei, “An Identity-based Signature and its Threshold Version”, Proceedings of AINA-05, IEEE, 2005.