Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An ID-Based Threshold Signcryption Scheme with Threshold Unsigncryption

Tej Singh
Deptt. of Mathematics, IMS Engineering College, Ghaziabad, India

Rashid Ali
Deptt. of Mathematics, Krishna Engineering College, Ghaziabad, India

***Abstract*— *This paper presents an identity based threshold signcryption scheme with threshold unsigncryption. In this scheme any u or more members of the signcrypter group can cooperatively signcrypt the message, but u-1 or fewer members cannot. For unsigncryption, any third party can verify the validity of the signature, but to recover the message the cooperation of at least t members of the receivers group is required. The proposed scheme has the following advantages: it provides both public verifiability and forward security; the key management problem is simplified because of using ID-based cryptography*.**

***Keywords*— *Cryptography, identity-based cryptography, signcryption,(t, n) threshold, zero knowledge proof*.**

I. Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to "sign-then-encrypt" the message. Signcryption, first proposed by Zheng [24] in 1997, is a new cryptographic primitive that performs signature and encryption simultaneously, at much lower computational and communication overhead than the "sign-then-encrypt" approach.

However one shortcoming of Zheng's original scheme is that its non-repudiation procedure is inefficient since it is based on interactive zero-knowledge proof. To achieve simple and safe non-repudiation procedure, Bao and Deng [3] introduced a signcryption scheme that can be verified by a sender's public key. Jung et al. [11] discovered another weakness of Zheng's scheme when he showed that it does not provide forward security. Anyone who obtains the sender's private key can recover the original message of a signcrypted text. Steinfeld and Zheng [21] and Malone-Lee and Mao [17] proposed efficient signcryption schemes that are based on integer factorization and using RSA, respectively. The formal models and security proofs for signcryption schemes have been studied in [1].

Identity-based (ID-based) cryptosystem were introduced by Shamir [19].The unique property of ID-based cryptosystem is that a user's public key can be any binary string, such as an email address that can identify the user. This removes the need for senders to look up the recipient's public key before sending out an encrypted message. These systems involve a trusted authority called private key generators (PKG's) whose job is to compute user's private key from his/her identity information. In 2001 [4], Boneh & Franklin introduced identity-based encryption scheme using bilinear maps. Other id-based schemes using pairings were proposed after 2001 ([9],[22]).

First ID-based signcryption scheme was proposed by Malone-Lee [16] in 2002. Libert and Quisquater [13] pointed out that Malone-Lee's scheme is not semantically secure and proposed a provably secure ID-based signcryption schemes from pairings. However, the properties of public Verifiability and forward security are mutually exclusive in their scheme. Chow et al. [6] proposed ID-based signcryption schemes that provide both public verifiability and forward security. The first ID-based ring signcryption scheme was proposed in [10]. All of the above schemes consist of only single recipient. In 2002, Zhang et al. [23] proposed a new signcryption scheme with (t, n) shared unsigncryption in which at least t recipients must participate in an unsigncryption process. The scheme is based on discrete logarithm.

In 2004, Duan et al.'s [8] proposed an identity based threshold signcryption scheme by combining the concept of ID-based threshold signature and signcryption together. However, In Duan et al.'s [8], the master key of the PKG is distributed to a number of PKG's, which creates a bottleneck on the PKG's. In 2005, Peng and Li [18] proposed an ID-based threshold signcryption scheme based on Libert and Quisquater's ID-based signcryption scheme [12]. However, Peng and Li scheme [18] does not provide the forward security. That is, anyone who obtains the sender's private key can recover the original message of a signcrypted text. Ma et al.'s [15] also proposed a threshold signcryption scheme using the bilinear pairing. However, Ma et al.'s scheme [15] is not ID-based. In 2006, Fagen Li et al's [14] proposed an ID-based signcryption scheme with (t, n) shared unsigncryption.

In this paper, we propose an ID-based threshold signcryption scheme with threshold unsigncryption. In this scheme, any u or more members of the signcryption group can cooperatively signcrypt the message and any third party can verify the validity of the signature. However only t or more members, in the recipient group having n members can cooperatively recover the message.

As compared to Fagen Li et al's ID-based signcryption with (t,n) shared unsigncryption the proposed scheme avoids the misuse (abuse) of signcryption power. The proposed scheme has the following advantages: it provides both public verifiability and forward security. Further the scheme is ID-based therefore; the key management problem is simplified.

The rest of the paper is organized as follows: Some definitions and preliminary work are given in Section 2. Section 3 gives the general identity based threshold signcryption scheme. The proposed ID-based threshold signcryption scheme with threshold unsigncryption is given in section 4. The security of the scheme is discussed in Section 5. Finally, the conclusions are given in Section 6.

II. PRELIMINARIES

In this section, we briefly describe the basic definition and properties of bilinear pairings. The Shamir's *(t, n)* threshold scheme and Baek and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map are also briefly described. They are the basic tools to construct our scheme.

A. Bilinear Pairings

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, b be elements of Z_q^*. A bilinear pairings is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:

Bilinearity: For all P and Q Є G_1, e(aP, bQ) = e(P, Q)

Non-degeneracy: There exists P and Q Є G_1 such that $e(P, Q) \neq 1$.

Computability: There is an efficient algorithm to compute e(P, Q) for all P, Q Є G_1.

The security of our scheme described here relies on the hardness of the following problems:

1. Decisional Bilinear Diffie-Hellman Problem (DBDHP): Given two groups G_1 and G_2 of the same prime order q, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1 the Decisional Bilinear Diffie-Hellman problem (DBDHP) in (G_1, G_2, e) is to decide whether $h = e(P, P)^{abc}$ or not, given (P, aP, bP, cP) and an element h Є G_2.
2. Computation Bilinear Diffie-Hellman Problem (CBDHP): Given two groups G_1 and G_2 of the same prime order q, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Computational Bilinear Diffie-Hellman problem (CBDHP) in (G_1, G_2, e) is to compute $h = e(P, P)^{abc}$ given (P, aP, bP, cP).
3. Discrete Logarithm Problem (DLP): Given two group elements P and Q find an integer n, such that Q = nP whenever such an integer exists.
4. Gap Diffie-Hellman Groups: Groups where the CBDHP is hard but the DBDHP is easy. No algorithm is known to be able to solve any of them so far.

B. Shamir's (t, n) Threshold Scheme

In order to share a private key D_{ID}, we need the Shamir's (t, n) threshold scheme. Suppose that we have chosen integers t (a threshold) and n satisfying $1 \leq t \leq n \leq q$.

First, we pick $R_1, R_2 \ldots\ldots R_{t-1}$ at random from G_1^*. Then we construct a function $F(u) = D_{ID} + \sum_{j=1}^{t-1} u^j R_j$

Finally, we compute $D_{IDi} = F(i)$ for $1 \leq i \leq n$ and send D_{IDi} to the i^{th} member of the message recipient group. When the number of shares reaches the threshold t, the function F(u) can be reconstructed by computing $F(u) = \sum_{j=1}^{t} D_{ID_j} N_j$

where $N_j = \prod_{i=1, i \neq j}^{t} \frac{u-i}{j-i} \bmod q$. The private key D_{ID} can be recover by computing $D_{ID} = F(0)$.

C. Back and Zheng's zero knowledge proof for the equality of two discrete Logarithms based on the bilinear map

To ensure that all decryption shares are correct, that is, to give robustness to threshold unsigncryption, we need a certain checking procedure. We use the Back and Zheng's zero knowledge proof for the equality of two discrete logarithms based on the bilinear map for the language

$L_{EDLog_{P,\tilde{P}}^{G_2}} = \text{def} \left\{(\mu, \tilde{\mu}) \in G_2 \times G_2 \middle| \log_g \mu = \log_{\tilde{g}} \tilde{\mu}\right\}$ where g = e(P,P) and $\tilde{g} = e(P, \tilde{P})$ for generators P and $\tilde{P}$ of G_1 as follows:

Suppose that $(P, \tilde{P}, g, \tilde{g})$ and $(k, \tilde{k}) \in L_{EDLog_{P,\tilde{P}}^{G_2}}$ are given to the prover and the verifier, and the prover knows a secret S Є G_1. The proof system works as follows.

1. The prover chooses T from G_1 randomly and computes $r = e(T, P)$ and $\tilde{r} = e(T, \tilde{P})$. The prover sends r and $\tilde{r}$ to the verifier.
2. The verifier chooses h from Z_q^* randomly and sends it to the prover.
3. On receiving h, the prover computes $W = T + hS$ and sends it to the verifier.
4. The verifier checks if $e(W, P) = rk^h$ and $e(W, \tilde{P}) = \tilde{r}\tilde{k}^h$. If the equality holds then the verifier returns "Accept", otherwise, returns "Reject".

III. GENERAL IDENTITY BASED THRESHOLD SIGNCRYPTION

A generic identity-based threshold signcryption scheme with total n players and t threshold limit consists of the following five algorithms.

A. Setup: given a security parameter k, the private key generator (PKG) generates the systems public parameters params. Among the parameters produced by Setup is a key P_{pub} that is made public. There is also corresponding master key s that is kept secret.

B. Extract: Given an identity ID, the PKG computes the corresponding private key S_{ID} and transmits it to its owner in a secure way.

C. Keydis: Given a private key S_{ID} associated with an identity ID, the number of signcryption members n and a threshold parameter t, this algorithm generates n shares of S_{ID} and provides each one to the signcryption members M_1, M_2,…….,M_n. it is also generates a set of verification keys that can be used to check the validity of each shared private key. We denote the shared private keys and the matching verification keys by $\{S_i\}_{i=1,2…n}$ and $\{y_i\}_{i=1,2…n}$,respectively. Note that each (S_i, y_i) is sent to M_i, then M_i publishes y_i but keeps S_i secret.

D. Signcrypt: Given a message m, the private keys of t members $\{S_i\}_{i=1,2…t}$ in a sender group U_A with identity ID_A, a receiver's identity ID_B, it outputs an identity based (t, n) threshold signcryption σ on the message m.

E. Unsigncrypt: Give a ciphertext σ, the private key of thr receiver S_{IDB}, the identity of the sender group ID_A, it outputs the plain text m or the symbol $\perp$ if σ is an invalid ciphertext between the group U_A and the receiver. We make the considtency constraint that if σ = signcrypt (m, $\{S_i\}_{i=1,2,…n}$, $ID_{\mathbf{B}}$), then m=Unsigncrypt (σ, ID_A,S_{IDB}).

IV. OUR PROPOSED SCHEME

The proposed scheme involves three entities, the Private Key Generator (PKG), the group A consisting of senders A_1, A_2,…..A_m and the message recipient group L with n members L_1, L_2,…….L_n. Suppose we choose integers u (as a threshold) and m satisfying $1 \le u \le m < q$ also integers t (as a threshold) and n satisfying $1 \le t \le n < q$. Here message is signcrypted by any u members of the group A jointly and unsigncrypted by any t members of the recipient group L jointly.

*1) Set up***:** PKG chooses G_1 and G_2 of order q (prime), a generator P of G1.

$$e : G_1 \times G_1 \to G_2, H_1 : \{0,1\}^* \to G_1, H_2 : G_2 \to \{0,1\}^n \; H_3 : \{0,1\}^* \times G_2 \to Z_q^*, \text{ and } H_4 : G_2 \times G_2 \times G_2 \to Z_q^*.$$

PKG chooses a master key $s \in Z_q^*$ and computes P_{pub} = sP. It also chooses a secure symmetric cipher (E, D) the PKG publishes parameters {G_1, G_2, n, e, P, $P_{pub,}$ H_1, H_2, H_3, E, D} and keeps the master key s secret.

Extraction: The group A = {A_1, A_2,…….A_m} has a group public key $Q_{ID_A} = H_1(ID_A)$. PKG computes sender group A's private signcryption Key $S_{ID_A} = s^{-1}Q_{ID_A}$. Next PKG picks a_1, a_2……..a_{u-1} at random from G_1^* and constructs a function $f(x) = S_{ID_A} + \sum_{j=1}^{u-1} a_j x^j$. Then PKG computes the sub private signcryption keys S_{Ai} = f(i) and send to each member A_i of A secretly. The message recipient group L has a public key Q_{ID_L} and private decryption key $D_{ID_L} = sQ_{ID_L}$. Now PKG choose randomly R_1, R_2,…….R_{t-1} from G_1^* and constructs a function $F(y) = D_{ID_L} + \sum_{j=1}^{t-1} R_j y^j$.

Then PKG computes private key D_L = F(i) and verification key $y_i = e(D_L, P)$ for recipient L_i $(1 \le I \le n)$. PKG secretly sends the private key D_L to L_i and publishes the verification key y_i.

1) *Signcryption*: Without loss of generality we may let (A_1, A_2,….A_u) be the u member of the group A that want to cooperatively signcrypt the message.To send a message m to the recipient group L.

a. Each A_i randomly chooses $x_i \in Z_q^*$, computes $k_{1i} = e(P, Q_{ID_A})^{x_i}$ and $k_{2i} = e(Q_{ID_A}, Q_{ID_L})^{x_i}$ and send k_{1i} and k_{2i} to the other u-1 members.

b. Each A_i compute $k_1 = \prod_{i=1}^{u} k_{1i}$, $k_2 = H_2\left(\prod_{i=1}^{u} k_{2i}\right)$

$c = E_{k_2}(m)$, and $r = H_3(c, k_1)$.

c. Then all u members cooperatively compute

$$S = \left(\sum_{i=1}^{u} x_i - r\right)\sum_{i=1}^{u}\lambda_i S_{A_i} \qquad \text{Where } \lambda_i = \frac{\prod_{i=1,i\neq j}^{u} 0-i}{\prod_{i=1,i\neq j}^{u} j-i} \bmod q$$

$$= (x-r)\sum_{i=1}^{u}\lambda_i f(ID_i)$$

$$= (x-r)S_{ID_A}$$

Signcryption is (c,r,S).

2) *Unsigncryption*: Without loss of generality, let $L'=\{L_1, L_2,\ldots,L_t\}$ be the t members of L that want to cooperatively unsigncrypt the received signcrypted message (c,r,S).

For signature verification each $L_i \in L'$ computes $k_1' = e(S, P_{pub})e(Q_{ID_A}, P)^r$.

a. Accept the signature iff $r = H_3(c, k_1')$.

b. For decryption each $L_i \in L'$ computes $\tilde{y}_i = e(D_{L_i}, S)$ $\tilde{u}_i = e(T_i, S)$, $u_i = e(T_i, P)$, $v_i = H_4(\tilde{y}_i, \tilde{u}_i, u_i)$ and $W_i = T_i + v_i D_{L_i}$ for $T_i \in G_1$ and sends $\sigma_i = (i, \tilde{y}_i, \tilde{u}_i, u_i, v_i, W_i)$ to the other t-1 member in L'.

c. To check that $\sigma_j = (j, \tilde{y}_j, \tilde{u}_j, u_j, v_j, W_j)$ from L_j ($j \neq i$) is a valid decryption share, L_i computes $v_j' = H_4(\tilde{y}_j, \tilde{u}_j, u_j)$ and then checks if $v_j' = v_j$, $e(W_j, S) = \tilde{y}_j^{v_j'}\tilde{u}_j$ and $e(W_j, P) = y_j^{v_j'} u_j$.

d. To recover m all the t members cooperatively compute $k_2' = H_2\left(\prod_{j=1}^{t}\tilde{y}_j^{N_j} e(Q_{ID_A}, Q_{ID_L})^r\right)$

where $N_j = \prod_{i=1,i\neq j}^{t}\frac{0-i}{j-i} \bmod q$, and

e. Recover the message m as $D_{k_2'}(c)$.

V. ANALYSIS OF THE SCHEME

A. Correctness Proof

The correctness can be easily verified by the following equations.

$$k_1' = e(S, P_{PUB})e(Q_{ID_A}, P)^r$$

$$= e(xS_{ID_A}, P_{PUB})e(S_{ID_A}, P_{PUB})^{-r} e(Q_{ID_A}, P)^r$$

$$= e(P, Q_{ID_A})^x$$

$$k_2' = H_2(\prod_{j=1}^{t}\tilde{y}_j^{N_j} e(Q_{ID_A}, Q_{ID_L})^r)$$

$$= H_2(\prod_{j=1}^{t} e(N_j D_{L_j}, S)(Q_{ID_A}, Q_{ID_L})^r)$$

$$= H_2(e(\sum_{j=1}^{t} N_j D_{L_j}, S)e(Q_{ID_A}, Q_{ID_L})^r)$$

$$= H_2(e(D_{ID_L}, S)e(Q_{ID_A}, Q_{ID_L})^r)$$

$$= H_2(e(D_{ID_L}, xS_{ID_A})e(D_{ID_L}, S_{ID_A})^{-r} e(Q_{ID_A}, Q_{ID_L})^r)$$

$$= H_2(e(Q_{ID_A}, Q_{ID_L})^x)$$

B. Security Analysis

1. *Unforgeability*: Any entity out of the signcryption group or less than u members of the group to collaborate will not be able to forge a valid signcryption.

2. *Confidentiality*: In the unsigncryption phase, any t-1 or fewer recipients can not recover the k_2. Thus they canot recover the message. It is difficult to compute D_{L_i} from $\tilde{y}_i$ since it is difficult to invert the bilinear mapping. Dishonest reciepient cannot cheat others by presenting $\tilde{y}_i$ since we use the checking procedure based on the Baek and Zheng's zero knowledge proof for equality of two discrete logarithms based on the bilinear map.

3. *Public verifiability*: For signature verification we comput $k_1' = e(S, P_{PUB})e(Q_{ID_A}, P)^r$, since all the parameter are publicly known therefore any third party can verify the signature, so our scheme provides the public verifiability.

4. Forwad security: Even though S_{ID_A} is revealed, any third party cannot compute k'_2 without knowledge of D_{ID_L}. Therefore, our scheme provides the forward Security.

VI. CONCLUSION

In this paper, we construct a new ID-based threshold signcryption scheme with threshold unsigncryption from pairing. In the proposed scheme any u or more members of the signcryption group can cooperatively signcrypt the message and any third party can verify the validity of the signature but at least t members in the recipient group can cooperatively recover the message.

REFERENCES

[1] J. Baek, R. Steinfeld, and Y. Zheng, "*Formal proofs for the security of signcryption*", in *PKC 2002*, LNCS #2274, pp. 80-98, Springer- Verlag, 2002.

[2] J. Baek and Y. Zheng, "*Identity-based threshold decryption*", in *PKC 2004,* LNCS #294, pp. 262-2767, Springer-Verlag, 2004.

[3] F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key", in PKC'98, LNCS #1431, pp. 55-59, Springer-Verlag, 1998.

[4] D. Boneh and M. Franklin, "*Identity-based encryption from the weil pairing*", in *CRYPTO 2001,* LNCS #2139, pp. 213-229, Springer-Verlag, 2001.

[5] J. C.Cha, J.H.Cheon, "*An identity –based signature from Gap Diffie-Hellman groups*", in *PKC 2003*, Springer-Verlag, Lecture notes in Computer Science series.

[6] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity", in International Conference on Information Security and Cryptology (ICISC 2003), LNCS #2971, pp. 352-369, Springer-Verlag, 2003.

[7] X. Du, Y. Wang, J. Ge, and Y. Wang. "An ID-based broadcast encryption scheme for key distribution", IEEE Transactions on Broadcasting, vol. 51, no. 2, pp. 264-266, 2005.

[8] S. Duan, Z. Cao, and R. Lu," *Robust ID-based threshold signcryption scheme from pairings*", In Proc.2004 International conference on information security, pp.33-37, Shanghai, China, 2004.

[9] F. Hess, "Efficient identity based signature schemes based on pairings", in Selected Areas in Cryptography (SAC 2002), LNCS #2595, pp. 310-32, Springer-Verlag, 2003.

[10] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world", in 19th International Conference on Advanced Information Networking and Applications (AINA '05), pp. 649-654, Taipei, Taiwan, 2005.

[11] F. Y. Jung, D. H. Lee, J. I. Lim, and K. S. Chang, "Signcryption schemes with forward secrecy", in The Second Workshop Information Security Application (WISA 2001), pp. 463-475, Seoul, Korea, 2001.

[12] M. Kudo, "Secure electronic sealed-bid auction protocol with public key cryptography", IEICE Transactions on Fundamentals, vol. E81-A, no. 1, pp. 20-26, 1998.

[13] B. Libert and J. Quisquater, "A new identity based signcryption schemes from pairings", in 2003 IEEE Information Theory Workshop,pp. 155-158, Paris, France, 2003.

[14] Fagen Li, Xiangjun Xin , and Yupu Hu, "ID-based signcryption scheme with (t,n) shared unsigncryption" in International journal of Network Security, Vol.3,No.1, pp.64-68, july 2006.

[15] C. Ma, K. Chen, D. Zheng and S. Liu,"*Efficient and proactive threshold signcryption*", in Proc. Information Security Conference-ISC 2005, LNCS 3650, pp. 233-243, Springer –Verlag, 2005.

[16] F. Malone-Lee, "*Identity based signcryption*", *Cryp-tology ePrint Archive,*Report 2002/098, 2002. Available from: http://eprint.iacr.org/2002/098.

[17] F. Malone-Lee and W. Mao, "*Two birds one stone: signcryption using RSA*", in *Topics in Cryptology-CT-RSA 2003,* LNCS #2612, pp. 211-225, Springer-Verlag, 2003.

[18] C. Peng and X. Li, "*An identity-based threshold signcryption scheme with semantic security*", in Proc. Computational Intelligence and Security-CIS 2005, LNAI3802 pp. 173-179. Springer-Verlag 2005.

[19] A. Shamir, "*How to share a secret*", *Communications of the ACM,* vol. 24, no. 11, pp. 612-613, 1979.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes", in CRYPTO'84, LNCS #196, Springer-Verlag, pp. 47-53, 1984.

[21] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization", in The Third Information Security Workshop (ISW 2000), LNCS #1975, pp. 308-322, Springer-Verlag, 2000.

[22] N. P. Smart, "An identity based authenticated key agreement protocol based on the weil pairing", in Electronic Letters, 38(13):630-632, 2002.

[23] Z. Zhang, C. Mian, and Q. Jin, "Signcryption scheme with threshold shared unsigncryption preventing malicious receivers", in IEEE Region 10 Technical Conference on Computers, Communications, Control and Power Engineering (IEEE TENCON'02), pp. 196-199, Beijing, China, 2002.

[24] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption)", in CRYPTO'97, LNCS #1294, Springer-Verlag, pp. 165-179, 1997.