A note on the Certificateless Multi-receiver Signcryption Scheme

S. Sharmila Deva Selvi[1], S. Sree Vivek[1,⋆], C. Pandu Rangan[1,⋆]

[1]Department of Computer Science and Engineering,
Indian Institute of Technology Madras.
sharmila@cse.iitm.ac.in,svivek@cse.iitm.ac.in, prangan@iitm.ac.in.

Abstract. Certificateless cryptography aims at combining the advantages of identity based and public key cryptography, so as to avoid the key escrow problem inherent in the identity based system and cumbersome certificate management in public key infrastructure. Signcryption achieves confidentiality and authentication simultaneously in an efficient manner. Multi-receiver signcryption demands signcrypting the same message efficiently for a large number of receivers. In this note, we strengthen the security of the certificateless multi-receiver signcryption scheme in [23] by proposing suitable enhancement to the scheme.

Keywords. Certificateless, Signcryption, Multi-receiver, Bilinear Pairing, Cryptanalysis.

1 Introduction

Signcryption proposed by Zheng in [3] is a cryptographic primitive providing signature and encryption simultaneously, at a lower computational cost and communication overhead than the signature-then-encryption approach. A proper signcryption scheme should provide confidentiality as well as authentication and non-repudiation. Besides this, security model for signcryption should consider insider attacks also i.e. a corrupted receiver should not be able to forge a valid signcryption from any legal user A to another user B on a message that was not already sent from A to B. Sometimes forward secrecy is also a desired property, which requires that even if a sender's secret key is exposed at some point of time, the past messages sent by him should remain secret.

Need for multi-receiver signcryption arises when the same message is to be sent to a large number of receivers. Consider the case of a company in which there are several managers and each of them has to send authenticated and confidential report to a large number of employees. In this case, simply signcrypting the message for each receiver will be highly inefficient. Therefore, there is a need

⋆ Work supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation sponsored by Department of Information Technology, Government of India

to design efficient schemes for this task. In [23], an efficient multi-receiver signcryption scheme(CLMSC) in certificateless setting was proposed to achieve this functionality.
The certificateless multi receiver signcryption scheme in [23] is secure against Type-II adversary, but it does not resist TYPE-I adversary. Also, the Type-I forgeability is reported in [24]. In order to make it secure against the attacks we propose some enhancement to the existing scheme in [23].

2 Preliminaries

2.1 Computational Assumptions

In this section, we recall the computational assumptions related to bilinear maps [16] that are relevant to the security of our scheme:

1. **Strong Diffie-Hellman Problem (SDHP)** SDH problem is a stronger version of DHI(Diffie-Hellman Inversion problem)[16]. Given $(P, aP) \in \mathbb{G}_1^2$ for any random $a \in \mathbb{Z}_q^*$, the SDH problem in $\mathbb{G}_1$ is to compute $\big(h, (a+h)^{-1}P\big)$, $h \in \mathbb{Z}_Q^*$.
   The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the SDH problem in $\mathbb{G}_1$ is defined as:

$$Adv_{\mathcal{A}}^{SDH} = Pr\left[\mathcal{A}(P, aP) = \big(h, (a+h)^{-1}P\big) \mid a, h \in \mathbb{Z}_q^*\right]$$

   We say that SDH is (t, ϵ) hard if for any t time probabilistic algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{SDH} < \epsilon$.
2. **Collusion Attack Algorithm with k-traitors (k-CAA)** Given $(P, aP, (h_1+a)^{-1}P, \ldots, (h_k+a)^{-1}P) \in \mathbb{G}_1^{k+2}$ for any random $a \in \mathbb{Z}_q^*$ and known values $h_1, \ldots, h_k \in \mathbb{Z}_q^*$, the k-CAA problem in $\mathbb{G}_1$ is to compute $(a+h)^{-1}P$ for some $h \notin \{h_1, \ldots, h_k\}$.
   The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the k-CAA problem in $\mathbb{G}_1$ is defined as:

$$\begin{aligned} Adv_{\mathcal{A}}^{k-CAA} &= Pr[\mathcal{A}(P, aP, (h_1+a)^{-1}P, \ldots, (h_k+a)^{-1}P, h_1, \ldots, h_k) \\ &= (a+h)^{-1}P \mid a, h \in \mathbb{Z}_q^*, h \notin \{h_1, \ldots, h_k\}] \end{aligned}$$

   We say that k-CAA is (t, ϵ) hard if for any t time probabilistic algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{k-CAA} < \epsilon$.
3. **Modified BDHI for k-values (k-mBDHIP)** k-mBDHIP is the bilinear variant of the k-CAA problem [22]. Given $(P, sP, (h_1+s)^{-1}P, \ldots, (h_k+s)^{-1}P) \in \mathbb{G}_1^{k+2}$ for any random $s \in \mathbb{Z}_q^*$ and known values $h_1, \ldots, h_k \in \mathbb{Z}_q^*$, the k-mBDHIP problem is to compute $\hat{e}(P, P)^{(s+h)^{-1}}$ for some $h \notin \{h_1, \ldots, h_k\}$.
   The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the k-mBDHIP problem in is defined as:

$$Adv_{\mathcal{A}}^{k-mBDHIP} = Pr[\mathcal{A}(P, sP, (h_1+s)^{-1}P, \ldots, (h_k+s)^{-1}P, h_1, \ldots, h_k)$$

$$= \hat{e}(P,P)^{(s+h)^{-1}} \mid s,h \in \mathbb{Z}_q^*, h \notin \{h_1,\ldots,h_k\}]$$

We say that k-mBDHIP is (t,ϵ) hard if for any t time probabilistic algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{k-mBDHIP} < \epsilon$.

4. **Gap Bilinear Diffie-Hellman Problem (GBDHP)**[12] Given $(P, aP, bP, cP) \in \mathbb{G}_1^4$ for any random $a,b,c \in \mathbb{Z}_q^*$, the GBDH problem in $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ is to compute $\hat{e}(P,P)^{abc}$ given access to DBDH oracle $\mathcal{O}_\Gamma$ which on input $(P, aP, bP, cP, T) \in \mathbb{G}_1^4 \times \mathbb{G}_2$ outputs 1 if $T = \hat{e}(P,P)^{abc}$ and 0 otherwise. The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the GBDH problem in $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ is defined as:

$$Adv_{\mathcal{A}}^{GBDH}(\mathcal{O}_\Gamma, q_{DBDH}) = Pr\left[\mathcal{A}^{\mathcal{O}_\Gamma}(P,aP,bP,cP) = \hat{e}(P,P)^{abc} \mid a,b,c \in \mathbb{Z}_q^*\right]$$

where q_{DBDH} is the number of queries to the decisional oracle. We say that GBDHP is (t,ϵ,q_{DBDH}) hard if for any t time probabilistic algorithm $\mathcal{A}$ asking q_{DBDH} oracle queries, advantage $Adv_{\mathcal{A}}^{k-CAA} < \epsilon$.

3 Certificateless Multi-receiver Signcryption

3.1 Framework of Certificateless Multi-receiver Signcryption

Any generic certificateless multi-receiver signcryption scheme is a five tuple of probabilistic polynomial time algorithms defined as follows-

1. ***Setup***(1^κ): This algorithm is run by the KGC. It takes as input the security parameter 1^κ and returns the KGC's master secret key Msk, master public key Mpk, public parameters $Params$ and a description of message space($\mathcal{M}_{CLMSC}$) and cipher-text space ($\mathcal{C}_{CLMSC}$).
2. ***Partial Private Key Extract***$(ID_i, Msk, Params)$: This algorithm is run by the KGC. It takes as input $Msk, Params$, a string $ID_i \in \{0,1\}^*$ and returns a partial private key D_i.
3. ***Key Extract***$(ID_i, D_i, Params)$: This algorithm is run by the user. It takes as input the partial private key of the user and returns a public key PK_i and a secret value x_i. The full secret key of the user is set to $SK_i = \langle x_i, D_i \rangle$.
4. ***Signcrypt***$(m, ID_S, SK_S, PK_S, L = \{ID_1, ID_2, \ldots, ID_n\}, PK_1, \ldots, PK_n, Params)$: The signcryption algorithm takes as input a message $m \in \mathcal{M}_{CLMSC}$, identity ID_S and the full secret key SK_S of the sender, a list L of the receiver identities and their public keys and returns a ciphertext $\sigma \in \mathcal{C}_{CLMSC}$.
5. ***Designcrypt***$(\sigma, SK_R, ID_R, PK_R, ID_S, PK_S, L)$: This is a deterministic algorithm which takes as input the ciphertext σ, receivers full secret key SK_R, identity ID_R, the public key PK_R of the receiver, list of receivers L, the identity ID_S and the public key PK_S of the sender and returns either a plaintext $m \in \mathcal{M}_{CLMSC}$ or an error symbol $\perp$.

For consistency, we require that
if $\sigma = Signcrypt(m, ID_S, SK_S, PK_S, L = \{ID_{R_1}, \ldots, ID_{R_n}\}, PK_1, \ldots, PK_n, Params)$, then $m = Designcrypt(\sigma, SK_{R_i}, ID_{R_i}, PK_{R_i}, ID_S, PK_S, L)$ for $1 \leq i \leq n$.

3.2 Security Model For Certificateless Multi-receiver Signcryption

Now, we describe the security model for certificateless multi-receiver signcryption. In confidentiality and unforgeability game we provide access to the following six oracles :

1. ***Extract Partial Private Key:*** On input of an identity ID_i, this oracle returns the partial private key D_i generated using the *Partial Private Key Extract* algorithm.
2. ***Extract Secret Key:*** On input of an identity ID_i, this oracle returns the full secret key $SK_i = \langle x_i, D_i \rangle$ of the identity using the appropriate algorithms.
3. ***Request Public Key:*** On input of an identity ID_i, this oracle returns the corresponding public key PK_i associated with ID_i. If such a key does not exist then it is constructed using *Key Extract* algorithm.
4. ***Replace Public Key:*** On input of an identity ID_i and a valid public key PK_i', this oracle replaces the public key associated with ID_i with PK_i'. If such a key does not exist then it is generated using the *Key Extract* algorithm and then the public key corresponding to ID_i is replaced with PK_i'.
5. ***Signcrypt:*** On input of a message, a sender's identity ID_S and a set of receiver identities $L = \{ID_{R_1}, ID_{R_2}, \ldots, ID_{R_n}\}$, this oracle returns the result of running the signcryption algorithm on the message, sender's full secret key and the receiver's public parameters.
6. ***Designcrypt:*** On input of a ciphertext, a sender's identity ID_S and a receiver's identity ID_R, this oracle returns the result of running the *Designcrypt* algorithm on the ciphertext, the sender's public parameters and the receiver's full secret key.

Next, we give the security definitions. Following the trend in literature we also consider Type-I and Type-II adversary. Roughly speaking Type-I adversary models a common user who is not in possession of the master secret key Msk and a type-II adversary models the honest but curious KGC.

Confidentiality: Security game that captures the confidentiality is based on the ciphertext indistinguishability. We define it separately for Type-I and Type-II adversary:
Type-I: A certificateless multi-receiver signcryption scheme is Type-I-iCCA2 secure if every probabilistic polynomial-time attacker $\mathcal{A}$ has negligible advantage in winning the IND-CLMSC-iCCA2-I game. A type-I adversary is given access to all the 6 oracles defined above under the following constraints-

1. Adversary does not have access to master secret key Msk.
2. No *Extract Secret Key* query is allowed on any of the challenge identities.
3. Adversary is not allowed to ask *Extract Partial Private Key* query for any of the challenge identities.

IND-CLMSC-iCCA2-I game played between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ is defined below:
Setup: Challenger $\mathcal{C}$ runs the setup algorithm to generate master secret key Msk and public parameters $Params$. $\mathcal{C}$ gives $Params$ to $\mathcal{A}$ while keeping Msk secret. After receiving $Params$ $\mathcal{A}$ outputs list of target identities denoted by $L^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$ respectively. $\mathcal{C}$ interacts with $\mathcal{A}$ in two phases:
Phase1: $\mathcal{A}$ is given access to all the six oracles. $\mathcal{A}$ adaptively queries the oracles consistent with the constraints described above.
Challenge: $\mathcal{A}$ outputs two equal length messages m_0, m_1 and an arbitrary sender's identity ID_S. $\mathcal{C}$ randomly chooses a bit $b \in_R \{0,1\}$ and computes a signcryption

$$\sigma^* = Signcrypt\left(m_b, ID_S, SK_S, PK_S, L = \{ID_1^*, \ldots, ID_n^*\}, PK_1^*, \ldots, PK_n^*\right)$$

σ^* is sent to $\mathcal{A}$ as challenge.
Phase2:$\mathcal{A}$ adaptively queries the oracles consistent with the constraints described above. Besides this it cannot query *Designcrypt* on σ^* for any $ID \in \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$.
Guess: $\mathcal{A}$ outputs a bit b' at the end of the game. $\mathcal{A}$ wins if $b = b'$. The advantage of $\mathcal{A}$ is defined as-

$$Adv_{\mathcal{A}}^{IND-CLMSC-iCCA2-I} = |2Pr[b = b'] - 1|$$

Type-II: A certificateless multi-receiver signcryption scheme is Type-II-iCCA2 secure if every probabilistic polynomial-time attacker $\mathcal{A}$ has negligible advantage in winning the IND-CLMSC-iCCA2-II game. A type-II adversary is given access to all the 6 oracles defined above and master secret key Msk under the following constraints-

1. No *Extract Secret Key* query is allowed on any of the challenge identities.
2. No *Replace Public Key* query is allowed on any of the challenge identities before the challenge phase.

IND-CLMSC-iCCA2-II game played between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ is same as the IND-CLMSC-iCCA2-I game with the restrictions mentioned above
The advantage of $\mathcal{A}$ is defined as-

$$Adv_{\mathcal{A}}^{IND-CLMSC-iCCA2-II} = |2Pr[b = b'] - 1|$$

Authenticity: Strong existential unforgeability(sEUF-CLMSC-iCMA) game captures the authenticity as a security requirement for any certificateless multi-receiver signcryption. By strong unforgeability we mean that adversary should not be able to signcrypt a message on behalf of a sender even if it knows the secret keys of all the receivers. The game is defined as below :
Type-I: A certificateless multi-receiver signcryption scheme is Type-I-sEUF-iCMA secure if every probabilistic polynomial-time attacker $\mathcal{F}$ has negligible advantage in winning the sEUF-CLMSC-iCMA-I game. A type-I adversary is given access to all the 6 oracles defined above under the following constraints-

1. Adversary does not have access to master secret key Msk.
2. No *Extract Secret Key* query is allowed on any of the challenge identities.
3. Adversary is not allowed to ask *Extract Partial Private Key* query for any of the challenge identities.

sEUF-CLMSC-iCMA-I game played between the challenger $\mathcal{C}$ and the adversary $\mathcal{F}$ is defined below:
Setup: Challenger $\mathcal{C}$ runs the setup algorithm to generate master secret key Msk and public parameters $Params$. $\mathcal{C}$ gives $Params$ to $\mathcal{F}$ while keeping Msk secret. After receiving $Params$ $\mathcal{F}$ outputs list of target identities denoted by $L^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$ respectively. $\mathcal{C}$ interacts with $\mathcal{F}$ in two phases:
Attack: $\mathcal{F}$ is given access to all the six oracles. $\mathcal{F}$ adaptively queries the oracles consistent with the constraints described above.
Forgery: $\mathcal{F}$ outputs a signature σ^* and n arbitrary receiver's identities $L = \{ID_{R_1}, \ldots, ID_{R_n}\}$(there exists atleast one receiver ID_{R_i} such that, $ID_{R_i} \notin L^*$). $\mathcal{F}$ wins if $Designcrypt(\sigma^*, SK_{R_i}, ID_{R_i}, PK_{R_i}, ID_j^*, PK_j^*, L)$ returns m for $i, j \in \{1, \ldots, n\}$ and σ^* was not the output of any signcrypt query $Signcrypt(m, ID_i^*, L = \{ID_{R_1}, \ldots, ID_{R_n}\})$.That is, $\mathcal{F}$ wins if it outputs a valid signcryption from a target identity to the set of receiver identities L by itself.
$Adv_{\mathcal{F}}^{sEUF-CLMSC-iCMA-II}$ is defined as the probability that $\mathcal{F}$ wins the above game.
Type-II: A certificateless multi-receiver signcryption scheme is Type-II-sEUF-iCMA secure if every probabilistic polynomial-time attacker $\mathcal{F}$ has negligible advantage in winning the sEUF-CLMSC-iCMA-II game. A type-II adversary is given access to all the 6 oracles defined above and the master secret key Msk under the following constraints-

1. No *Extract Secret Key* query is allowed on any of the challenge identities.
2. Adversary is not allowed to ask *Replace Public Key* for any of the challenge identities.

sEUF-CLMSC-iCMA-II game played between the challenger $\mathcal{C}$ and the adversary $\mathcal{F}$ is same as sEUF-CLMSC-iCMA-I with the restrictions given above.
$Adv_{\mathcal{F}}^{sEUF-CLMSC-iCMA-II}$ is defined as the probability that $\mathcal{F}$ wins the sEUF-CLMSC-iCMA-II game.

4 Enhancement of the Scheme in [23]

The scheme in [23] doesnot resist type-I adversary. When the adversary sees any signcryption $\sigma = \langle c, d_1, d_2, \ldots, d_n, L\rangle$ from ID_S to $L = \{ID_1, \ldots, ID_n\}$. The adversary can perform the following,
$d = d_{i1} - d_{j1}$, $ID_i, ID - j \in L$
$= r_1 P$
Knowing $d = r_1 P$ the type-I adversary can compute both the keys used for encryption namely $\hat{e}(P, Q)^{r_1} = \hat{e}(d, Q)$ and $(\hat{e}(P, Q)^{r_1})^{x_i}$, because the type-I adversary knows the secre value x_i and P,Q are public parameters. This is possible

because of the randomness being re-used in the computation of d_{i1} of all receivers. Hence, we overcome the weaaknes by performing the following enhancement,

Setup(1^κ)***:*** On providing security parameter 1^κ as input, the KGC chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q, two random generators P and Q of $\mathbb{G}_1$ such that $P \neq Q$ and a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. It then computes $g = \hat{e}(P, Q) \in \mathbb{G}_2$ and defines five hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_2 \times \{0,1\}^* \to \mathbb{Z}_q^*$, $H_3 : \{0,1\}^m \times \mathbb{G}_2 \times \{0,1\}^* \times \mathbb{G}_2 \times \mathbb{G}_1 \times \{0,1\}^* \to \mathbb{Z}_q^*$, $H_4 : \mathbb{Z}_q^* \times \{0,1\}^* \to \{0,1\}^{k_1+l_m}$, $H_5 : \mathbb{G}_2 \times \mathbb{G}_2 \times \mathbb{G}_2 \times \{0,1\}^* \to \{0,1\}^{k_1+k_2}$, where k_1, k_2 and l_m are the number of bits required to represent $\mathbb{G}_1$ elements, $\mathbb{Z}_q^*$ elements and message respectively. Then KGC chooses $s \in_R \mathbb{Z}_q^*$ as the master secret key and sets $P_{pub} = sP$. The KGC now publishes the public parameters $Params$ of the system as $\langle \mathbb{G}_1, \mathbb{G}_2, P, Q, P_{pub}, \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2, g, H_1, H_2, H_3, H_4, H_5 \rangle$.

Partial Private Key Extract(*ID_i, msk, $Params$****):*** On input ID_i, the partial private key of user with identity ID_i is computed as $D_i = (q_i + s)^{-1} Q$, where $q_i = H_1(ID_i)$.

Key Extract(*ID_i, D_i, $Params$****):*** This algorithm is run by each user to compute his private and public keys. The user ID_i chooses $x_i \in_R \mathbb{Z}_q^*$ and sets his private key $SK_i = \langle x_i, D_i \rangle$ and sets his public key as $Pk_i = \langle PK_{i1}, PK_{i2} \rangle = \langle g^{x_i}, x_i T_i \rangle$, where $T_i = (q_i + s)P$.

Signcrypt(*$m, ID_S, SK_S, PK_S, L = \{ID_{R_1}, ID_{R_2}, \ldots, ID_{R_n}\}$, $PK_{R_1}, PK_{R_2}, \ldots, PK_{R_n}, Params$****):***

1. Choose $r \in_R \mathbb{Z}_q^*$ and compute $\alpha = rP$
2. $h = H_2(\alpha, m, ID_S, L)$ and $h_3 = H_3(m, \alpha, h, ID_S, PK_{S1}, PK_{S2}, L)$
3. Compute $Z_S = \dfrac{r}{(x_S + h_3)} D_S$
4. Compute $c = H_4(h, ID_S, L) \oplus m \| \alpha$
5. Repeat the following steps for all $ID_{R_i} \in L$, $i = 1, 2, \ldots, n$.
   (a) Choose $r_i \in \mathbb{Z}_q^*$
   (b) Parse PK_{R_i} as $\langle PK_{i1}, PK_{i2} \rangle$
   (c) Set $h_{5i} = H_5(g^{r_i}, (PK_{i1})^{r_i}, PK_{i1}, ID_{R_i})$
   (d) Compute $d_{i1} = r_i(q_i + s)P$ and $d_{i2} = h_{5i} \oplus h \| Z_S$
   (e) Set $d_i = \langle d_{i1}, d_{i2} \rangle$
6. Return ciphertext $\sigma = \langle c, d_1, d_2, \ldots, d_n, L \rangle$.

Designcrypt(*$\sigma = \langle c, d_1, d_2, \ldots, d_n, L \rangle, ID_S, ID_i, SK_i, Params$****):***

1. Parse d_i as $\langle d_{i1}, d_{i2} \rangle$ and SK_i as $\langle x_i, D_i \rangle$
2. Compute $\omega' = \hat{e}(d_{i1}, D_i)$ and $(\omega')^{x_i} = (PK_{i1})^{r_i}$
3. Set $h'_{5i} = H_5(\omega', (\omega')^{x_i}, PK_{i1}, ID_i)$
4. Compute $h' \| Z'_S = h'_{5i} \oplus d_{i2}$
5. Compute $m' \| \alpha' = c \oplus H_4(h', ID_S, L)$
6. Set $h'_3 = H_3(m', \alpha', h', ID_S, PK_{S1}, PK_{S2}, L)$
7. If $h' \stackrel{?}{=} H_2(\alpha', ID_S, L)$ and $\hat{e}(PK_{S2} + h'_3(q_S + s)P, Z'_S) = \hat{e}(\alpha', Q)$ then return m', else return $\perp$.

5 Conclusion

We have proposed an enhancement for the security weakness in the certificateless signcryption scheme for multiple receivers in [23].

References

1. S.S. Al-Riyami and K.G. Paterson.: *Certificateless Public-Key Cryptography.* In: Advances in Cryptology ASIACRYPT 2003, LNCS 2894:452473, Springer-Verlag, 2003.
2. Yong Yu, Bo Yang, Xinyi Huang and Mingwu Zhang.: *Efficient identity-based signcryption scheme for multiple receivers.* In: ATC 2007, LNCS 4610, pp. 13-21, Springer-Verlag Berlin Heidelberg, 2007.
3. Zheng Y.: *Digital signcryption or How to achieve cost (signature & Encrytpion) ≪ cost(signature) + cost(encryption).* In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS vol. 1294, pp. 165-179. Springer, Heidelberg 1997.
4. Malone-Lee J., Mao M: *Two birds one stone: signcryption using RSA.* In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol.2612, pp. 211-226. Springer, Heidelberg 2003.
5. Malone-Lee J.: *Identity based signcryption.* In: Cryptology ePrint Archive. Report 2002/098, 2002.
6. Libert B., Quisquator J.J.: *A new identity based signcryption scheme from pairings.* In: 2003 IEEE information theory workshop.Paris, France, pp.155-158, 2003.
7. Boyen X.: *Multipurpose identity based signcryption: a swiss army knife for identity based cryptography.* In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 383-399. Springer, Heidelberg 2003.
8. Barreto P.S.L.M., Libert B., McCullagh N., Quisquater J.J.: *Efficient and provably-secure identity based signatures and signcryption from bilinear maps.* In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 515-532. Springer, Heidelberg 2005.
9. Zheng Y.: *Signcryption and its applications in efficient public key solutions.* In: Okamoto, E. (ed.) ISW 1997. LNCS, vol. 1396, pp. 291-312. Springer, Heidelberg 1998.
10. Duan S., Cao Z.: *Efficient and provably secure multi-receiver identity-based signcryption.* In: Batten, L.M., Safavi-Naini, R. (eds) ACISP 2006. LNCS, vol. 4058, pp. 195-206. Springer, Heidelberg 2006.
11. K. Kurosawa: *Multi-recipient public-key encryption with shortened ciphertext* In: Public Key Cryptography, 2002, pp. 48-63.
12. M. Barbosa and P. Farshim: *Certificateless Signcryption* In: Conference on Computer and Communications Security archive Proceedings of the 2008 ACM symposium on Information, Computer and Communications Security.
13. S. Sharmila Deva Selvi, S. Sree Vivek, Ragavendran Gopalakrishnan, Naga Naresh Karuturi and C. Pandu Rangan: *Cryptanalysis of ID-Based Signcryption Scheme for Multiple Receivers.* In: http://eprint.iacr.org/2008/238.pdf
14. R. Canetti, S. Halevi, J. Katz:*A forward-secure public-key encryption scheme* In: EUROCRYPT, 2003, pp. 255-271.
15. J.Baek, R. Naini, W.Susilo:*Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption* In:Springer Berlin Heidelberg ISSN 0302-9743 (Print) 1611-3349 (Online) Volume 4058/2006.

16. Ratna Dutta, Rana Barua and Palash Sarkar :*Pairing-Based Cryptographic Protocols : A Survey*. In http://eprint.iacr.org/2004/064.pdf.
17. Baek J., Steinfeld R., Zheng Y.: *Formal proofs for the security of signcryption.*. In:Public Key Cryptography - PKC 2002, volume 2274 of Lecture Notes in Computer Science, pages 80-98. Springer-Verlag, 2002.
18. M. Bellare, A. Boldyreva, S. Micali:*Public-key encryption in a multi-user setting: Security proofs and improvements*In: B. Preneel (Ed.), Advances in Cryptology EUROCRYPT 2000, Vol. 1807 of Lecture Notes in Computer Science, Springer-Verlag, Berlin Germany, Brugge, Belgium, 2000, pp. 259-274.
19. Alexander W. Dent :*A Survey of Certificateless Encryption Schemes and Security Models* In : eprint.iacr.org/2006/211.pdf.
20. Alexander W. Dent, Benoit Libert, Kenneth G. Paterson:*Certificateless Encryption Schemes Strongly Secure in the Standard Model*: In R. Cramer, editor(s), 11th International Workshop on Practice and Theory in Public-Key Cryptography (PKC 2008), Volume 4939 of Lecture Notes in Computer Science, pages 344-359, Springer, March 2008.
21. Benoit Libert, Jean-Jacques Quisquater:*On Constructing Certificateless Cryptosystems from Identity Based Encryption*, In : M. Yung, editor(s), Public Key Cryptography 2006 (PKC'06), Volume 3958 of Lecture Notes in Computer Science, pages 474-490, Springer, April 2006.
22. Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu and K.P. Chow :*Two Improved Partially Blind Signature Schemes from Bilinear Pairings*, In *Information Security and Privacy*, Volume 3574/2005 of *LNCS*, Pages 316-328. Springer. 2005
23. S. Sharmila Deva Selvi, S. Sree Vivek, Deepanshu Shukla and C. Pandu Rangan :*Efficient and Provably Secure Certificateless Multi-receiver Signcryption*In *Provable Security*, Volume 5324/2008 of *LNCS*, Pages 52-67, Springer, 2008.
24. Songqin Miao, Futai Zhang, Lei Zhang:*Cryptanalysis of a Certificateless Multi-receiver Signcryption Scheme*In *Multimedia Information Networking and Security (MINES), 2010*, pages 593 -597, 2008