http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (11): 2098-2104, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.2098.2104

A Short Identity-based Signcryption Scheme in the Multi-PKG over the VANETs

[1]Jianhong Zhang, [2]Yuanbo Cui and [1]Xiuna Su
[1]College of Sciences, North China University of Technology, Beijing, China
[2]Institution of Imagine Process and Pattern Recognition, North China University of Technology, Beijing, 100144, China

Abstract: Signcryption is a novel cryptographic primitive that simultaneously provides the authentication and encryption in a single logic step. In this study, by combining two ID-based signature schemes with a signcryption scheme, we build security model of ID-based signcryption in the multi-PKG and have proposed an ID-based signcryption scheme in the multi-PKG based on the bilinear pairings to adapt to the different crypto graphical system setting. We prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability. The fixed verification computation is needed in our proposed signcrypiton, thus, it is very efficient.

Key words: Signcryption, ID-based cryptography, security proof, the CDH problem

INTRODUCTION

A Vehicular Ad-Hoc Network(VANET), is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 m of each other to connect and in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. Thus, we adopt signcryption to realize security authentication and secret transmission.

Message security and the sender's identity authentication for communication in the open channel is a basic and important technology of internet. For keeping message confidential and unforgeable, the sender can use a digital sig nature algorithm with his private key to sign the message, then encrypts the message and its signature by a symmetric encryption algorithm with secret key. The sender encrypts this secret key with using the recipient's public key. The process is a sign-then-encrypt way to realize authentication and encryption. But computational costs and communication overheads are large in this way. Zheng (1997) first proposed a new cryptographic primitive: signcryption, which can perform digital signature and public key encryption in a logic step, at lower computational costs and communication overheads than the above sign-then-encrypt way. Since then, there are many signcryption schemes proposed.

It is only recently that a formal security proof model (Baek *et al*., 2002) is formalized providing security proof for Zheng (1997) in the random oracle model. By combining ID-based cryptology and signcryption, Malone-Lee (2002) proposed a first ID-based signcryption scheme. But Libert and Quisquater (2003) pointed out that Malone-Lee's scheme (Malone-Lee, 2002) is not

Corresponding Author: Yuanbo Cui, College of Sciences, North China University of Technology, Beijing, China

semantically secure, since the signature of the message is visible in the signcrypted message. Chow *et al.* (2004) proposed an ID-based signcryption scheme that can provide both public verifiability a forward security. In Boyen (2003) proposed a secure identity-based signcryption scheme with ciphertext anonymity and provable secure in the random oracle model.

Their security proof model is slightly di®erent from that of (Baek *et al.*, 2002) which includes the ciphertext anonymity. In Libert and Quisquater (2004) modified Boyen's security proof model to non-dentity based signcryption scheme and proposed a signcryption scheme. They proved that their signcryption scheme is secure in the random oracle model with the following properties: semantically security against adaptive chosen ciphertext attacks, ciphertext anonymity and key invisibility. Unfortunately, Tan showed that the scheme did not satisfy the above properties in Tan (2005). Up to now, the most efficient ID-based signcryption scheme (Barreto *et al.*, 2005) was proposed by Barreto *et al.* (2005) and the security of the scheme was based on recently studied computational assumptions: the q-Bilinear Diffie-Hellman Inversion problem.

In the cloud computing, grid computing, trust management is a crucial approach to authenticate user and protect resource. Trust between two unknown parties in different autonomous domain is established based on the party's properties, by which are proven their qualifications through the disclosure of appropriate credentials. Assertion, described as well-defined uniformly semantic structure entities such as credentials, policies and requests, is encrypted by issuer or authorities public key. In order to protect the security of assertion for decentralized autonomous environments, Zhang *et al.* (2008) proposed an efficient assertion security protect model based on signcryption scheme for multiple autonomous domain managers and Privacy Key Generators (PKGs). Unfortunately, Wang and Qian (2010) shown that their extensions were incorrect, i.e., Zhang *et al.* (2008) scheme is not suitable for multi-PKG scenario, it can reach consistency when only one PKG exists in the system. In this work, by combining two ID-based signature schemes with a signcryption scheme, we build security model of ID-based signcryption in the multi-PKG and have proposed an ID-based signcryption scheme in the multi-PKG based on the bilinear pairings to adapt to the different cryptographical system setting. We prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability.

PRELIMINARIES

Here, we briefly review the basic definition and properties of the bilinear pairings.

Let G_1 be a cyclic additive group generated by the generator P, whose order is a prime q and G_2 be a cyclic multiplicative group of the same prime order q.

We assume that the Discrete Logarithm Problem (DLP) in both G_1 and G_2 are hard. An admissible pairing e: $G_1 \times G_1 \rightarrow G_2$, which satisfies the following three properties:

- **Bilinear:** If P, $Q \in G_1$ and a, b $\in Z_q$, then e (aP, bP) = e (p, Q)^{ab}
- **Non-degenerate:** There exists a $P \in G_1$ such that e (P, P)$\neq$1
- **Computable:** If P, $Q \in G_1$, one can compute e (P, Q) $\in$ G_2 in the polynomial time

We note the modified Weil and Tate pairings associated with supersingular elliptic curves are examples of such admissible pairings. The security of the ID-based signcryption scheme discussed in this paper is based on the following security assumption.

Definition 1: Given two group 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 (DBHP) in (G_1, G_2, e) is to decide whether h = e (P, P)^{abc} given (P, aP, bP, cP) and an element $h \in G_2$. We define the advantage of a distinguisher against the DBDHP as follows:

$$AdvD = |P_{a,b,c\in Z_q, h\in G_2}[1 \leftarrow D(aP, bP, cP, h)] - P_{a,b,c\in Z_q}[1 \leftarrow D(aP, bP, cP, e(P,P)^{abc})]|$$

Definition 2: (CDH Assumption). Let gen be a CDH parameter generator. We say algorithm A has advantage $\varepsilon(k)$ in solving the CDH problem for gen if for a sufficiently large k

$$Adv_{gen,A}(t) = Pr[A(q, G_1, xP, yP) = xyP \mid (q, G_1) \leftarrow gen^k, P \leftarrow G_1, x, y \leftarrow Z_q]$$

We say that gen satisfies the CDH assumption if for any randomized polynomial time in t algorithm A we have the $Adv_{gen, A}(t)$ is negligible function.

DEFINITION AND SECURITY MODEL OF ID-BASED SIGNCRYPTION IN THE MULTI-PKG

An ID-based signcryption scheme in the multi-PKG consists of the algorithms <System Setup, PKG setup, Key Extract, Signcrypt, Unsigncrypt>. Malone-Lee (2002) define the security requirements for ID-based signcryption schemes. These security requirements include indistinguishable against adaptive chosen ciphertrext attacks and unforgeability against adaptive chosen message attacks. In the following, we modify his

definitions to adapt for our ID-based signcryption scheme in the multi-PKG.

System parameter setup: It takes a security parameter k as inputand returns system parameters Params. PKG- Setup: Each autonomous domain manager PKGi takes the *Params*as input and returns his public/private key pair (P^1_{pub}, s_i) where he only publishes his public key to group members.

Key extract: This algorithm is to produce a secret key SID of the user with identity ID, the method is the same a the ordinary ID-based key extract algorithm (Libert and Quisquater, 2003; Malone-Lee, 2000), where the difference is in that a user should register in and extract from his autonomous domain manager PKGi in multiple autonomous trust domain environments.

Signcrypt: To send an assertion a to Bob identified by IDB, the sender Alice produces the ciphertextσ by this algorithm on input of (a, S_A, ID_B, P^1_{pub}, P^2_{pub}).

Designcrypt: The recipient Bob with secret key SB under the different domain uses this algorithm to decrypt the ciphertext and verify the valid of the signature.

Definition 3: (Confidentiality) An ID-based signcryption scheme in the multi-PKG is indistinguishable against adaptive chosen ciphertext attacks property (IND-IDSCMP-CCA2) if no polynomial bounded adversary has a non-negligible advantage in the following game.

Setup: The challenger *C* runs Setup algorithm and Issuer-Setup algorithm with a security parameter k and sends the system parameters to the adversary A.

Phase 1: A performs a series of queries in an adaptive fashion. The following queries are allowed:

Key extraction queries: A chooses an identity ID. C computes private key s_{ID}, ID_B, P^1_{pub}, P^2_{pub} to response A.

Signcryption queries: A inputs the sender's identity ID_A and the recipient's identity ID_B and a signcrypt -ed message m, C computes σ = signurpt (m, s_{IDA}, ID_B, P^1_{pub}, P^2_{pub}) and sends it to A.

Unsigncryption queries: Given a ciphertext δ, the challenger C runs Unsigncrypt algorithm on input (δ, s_{IDB}, ID_A, P^1_{pub}, P^2_{pub}) and returns its output to A.

Selection: At the end of phase 1, A generates two equal length plaintext m_0 and m_1 and a sender's identity ID_A and the recipient ID_B on which he wants to be challenged. He cannot have query the private key of ID_B as the first phase.

Challenge: The challenge flips b $\in$ {0, 1} then computes δ = signcryption (s_{IDA}, ID_B, P^1_{pub}, P^2_{pub}) to return it to the adversary A.

Phase 2: A can ask a polynomial bounded number of queries adaptively again as in the first phase. But he cannot make a key extraction query on ID_B and cannot make an unsigncryption query on δ^*.

Output: A outputs a bit b′ and wins the game if b′ = b.

The advantage of A is defined as AdvA = |2P (b′ = b)-1|, where, P (b′ = b) denotes the probability that b′ = b.

Definition 4: Unforgeability: A signcryption scheme based on multiple PKGs is existentially unforgeable against chosen-message insider attack (EUF-IDASC-CMA2) if no PPT forger F has a non-negligible advantage in the following game:

- Challenger runs System. setup and Issuer. setup just like in IDASC game
- Forger F adaptively performs a number of queries just like in IDASC game
- F produces a ciphertext (δ, ID_A, ID_B) in the sense that the key is the range of key extract algorithm and wins the game if: (a) Designcrypt (δ; ID_A; ID_B) $\neq \perp$; (b) δ is not produced by Signcrypt oracle

OUR SCHEME

In this section, we give a novel ID-based signcryption scheme which is suitable to the multi-PKG. The details of our scheme are described as follows:

Setup: Given a security parameter *k*, select two bilinear map groups (G_1, G_2) of prime order $q > 2^k$, e: $G_1 \times G_1 \rightarrow G_2$and a generator $P \in_R G_1$. Define three hash functions H_i: $\{0, 1\}^* \rightarrow G_1$, H_2: $G_1 \times G_2$ and H_3: $G_2 \rightarrow G_1 \times \{0, 1\}^l$ where, l denotes the length of assertion *a*. Publish the system parameters (G_1, G_2, q, e, P, H_1, H_2, H_3). For each PKG_i, it randomly chooses $s_i \in Z_q$ to compute $P^1_{pub} = s_1P$ as his public key and secretly keeps s_i as his master key.

Key extraction: When a user registers his identity ID to PKG_i, the PKG_i computes $S_{ID} = s_1 Q_{ID}$ as the corresponding

secret key of the user ID where, $Q_{ID} = H_1(ID)$. Finally, PKG_1 sends the secret key S_{ID} to the user via a secure channel.

Signcryption: Given a message m, a recipient Bob's identity ID_B which secret key is issued by PKG_2, the sender Alice's secret key is issued by PKG_1. Note that the sender and recipient are the two users of different domains. Alice computes as follows:

- First, Alice send an assertion a to Bob with identity ID_B in trust domain PKG_2
- Then, it randomly chooses $r \in Z_q$ to compute $U = rP$
- Compute $h = H_2(U\|a\|m)$ and $V = rP^1_{pub} + hS_A$
- Compute $t = e(rP^2_{pub}, Q_B)$ and $W = H_3(t) \oplus (V\|Q_A\|a\|m)$
- Finally, the resultant ciphertext is $C = (U, W)$

De-signcryption: Upon receiving a ciphertext $C = (U, W)$ the recipient Bob does as follows:

- Firstly, the recipient Bob checks whether U belongs to group G_1, if it holds, then Bob computes $t = e(U, S_B)$
- Then recover $(V\|Q_A\|a\|m) = W \oplus H_3(t)$ and compute $h = H_2(U\|a\|m)$
- If $Q_A \notin G_1$ or $V \notin G_1$, then abort it. Otherwise, accept the assertion *a* and return TRUE if and only if the following equation holds

$$e(P,V) = e(P, rP^1_{pub} + hS_A) = e(P^1_{pub}, U + hQ_A)$$

If so, output valid; if not, output invalid.

SECURITY ANALYSIS

Theorem 1: (Confidentiality) Assume that an IND-IBSC-CCA adversary A has an advantage ε against our proposed scheme when running in time τ, asking q_{Hi} queries to random oracles H_i (i = 1, 2, 3), q_{se} signcryption queries and q_{us} queries to the unsigncryption oracle. Then there is an algorithm B to solve the DBDH problem with non-negligible probability.

Proof: Given a random instance (P, aP, bP, cP, h) of the Decisional Bilinear Diffie-Hellman problem, where $h \in G1$, we are going to construct a probabilistic polynomial time Turing machine D which use the attacker A as a subroutine in order to distinguish whether $h = e(P; P)^{abc}$ holds or not. In the whole game, A will consult D for answers to the random oracles H_1, H_2 and H3. And D needs to maintain hash lists L1; L2 and L3 that are initially empty and are used to keep track of answers to queries asked by A to oracle H1; H2 and H3.

We suppose that the following assumption are made:

- A asks for $H_1(ID)$ before ID is used in any key extraction query, signcryption query and unsigncryption query
- Ciphertext returned from a signacryption query will not be used by A in an unsigncryption query

At the beginning of the game, D randomly chooses $s_1 \in Z_q$ to compute $P^1_{pub} = s_1P$ as the public key of PKG_1 and sets the public key of PKG_2 with $P^2_{pub} = aP$ and sends (P^1_{pub}, P^2_{pub}) to the adversary A. (Note that a is unknown to D and plays the roles of PKG_2's master key in the game.) The identities of n signers are denoted by ID_{A1}, ID_{A2}, ...ID_{A3}. D chooses a random number $i \in \{1, 2,..., q_{H1}\}$ as challenged identity index.

Phase 1: A performs a first series of queries of the following kinds that are handled by D as explained below:

H_1-Oracles: When A asks H_1 queries with ID_j, D responses as follows:

- If j = i, then A answers by $H_1(Id_j) = bP$
- If $j \neq i$, then A randomly chooses $b_j \in Z_q$ to set $H_1(ID_1) = b_j P$ and records the pair (ID_j, b_j) in the list L_1

H_2-oracles: When A makes queries on H_2-oracle with w_j, D searches the pair (w_j, t_j) in the list L_2, if such a pair exists, then D responses t_j to A, otherwise, D randomly chooses $t_j \in Z_q$ to answer A and records this pair (w_j, t_j) in the list L2.

H_3-oracles: When A makes queries on H_3-oracle with t_j, D searches the pair (a_j, t_j) in the list L_2, if such a pair exists, then D responses α_j to A, otherwise, D randomly chooses $a_j \in Z_q$ to answer A and records this pair (a_j, t_j) in the list L_3.

Key extract oracle: When *A* makes a key extract query with ID_j to PKG_2, if j = i, then D fails and aborts it. Otherwise, D first searches ID_j in the list L_1. If the pair (ID_j, b_j) exists, then D responses $S_{IDj} = b_j P_{pub}$ as the private key, otherwise, he randomly selects $b_j \in Z_q$ to answer the private key $S_{IDJ} = b_j P_{pub}$ and records (ID_j, b_j) in the list L1.

When the adversary A makes a key extract query with ID_j to PKG1, D can use the master secret key s_j of PKG1 to compute the secret key $S_j = s_1 Q_A$, where $Q_A = H_1(ID_j)$ since it has PKG_1's master secret key.

Signcryption oracle: When an adversary makes a signcryption query with the message (ID_A, ID_B, M), D responses as follows:

For $ID_A \in \{0, 1\}^*$ which belongs to the domain of PKG_1, D has the master secret key of PKG_1 so that D can compute the secret key of the user with identity ID_A. It

means that D can use the secret key of ID_A to compute a ciphertext on message M.

Unsigncryption oracle: When A makes a unsigncryption query for $\delta = (U_1, U_2, W)$ from ID_A to ID_B. We consider the following cases:

- If $ID_B = ID_j$, D always answer A the δ is a valid ciphertext
- If $ID_B \in ID_j$, D can query key extract oracle with ID_B, thus, it can compute the secret key of the user with identity ID_B to recover the message m. Finally, D can recover V to check whether the following equation holds or not

$$e(P, V) = e(P^1_{pub}, U_2 + hQ_A)$$

Challenge: Finally, A outputs two equal length plaintexts m_0 and m_1 together with the receiver's secret key s_{ID_i} on which he wishes to be challenged. D randomly chooses $b \in \{0, 1\}$ and signcrypt m_b as follows:

- Set $U^* = cP$
- Compute $h^*_3 = H_3(t)$, where t is among the DBDH problem
- Compue $h^* = H(U^* \| Q_A \| a \| m_b)$

Finally, D sends the ciphertext $\delta^* = (U^*, W^*)$ to A.

Phase 2: A performs new queries which are treated in the same way of Phase 1. At the end of the simulation, it produces a bit b′ for its guess. If b = b′, then it denotes that D can output

$$t = e(U^*, s_{ID_i}) = e(cP, abP) = e(P, P)^{abc}$$

as a solution of distinguish DBDH problem, otherwise D outputs "failure".

Theorem 2: Suppose that there exists an adaptively chosen message and identity attack F making q_{HI} queries to random oracles H_i (i = 1, 2, 3), q_e queries to key extract oracle and q_s queries to the signcryption oracle. If the adversary F can produce a forgery with non-negligible probability, then, there exists an algorithm B which is able to solve the CDH problem.

Proof: Suppose that F is a forger which is able to break our proposed ID-based signcryption scheme. Given a CDH instance (P, xP, yP) $(x, y \in_R Z_q)$, we will construct an algorithm B to compute the CDH solution xyP in G_1 by using the algorithm F as subroutine. To do so, algorithm B performs the following simulation by interacting with the forger F.

Setup: Algorithm B sets the system-wide PKG_1's public key as $P^1_{pub} = xP$ and randomly chooses $s_2 \in Z_q$ to compute $P^2_{pub} = s_2P$ as the public key of PKG_2. Finally, B sends them to the adversary F.

At any time, algorithm A can query the random oracles H_1, H_2, H_3, Extract oracle and Signcryption Oracle. To answer these queries, B executes the following response.

H_1-queries: To respond to H_1-queries, the algorithm B maintains a list of tuples (ID, w, b, c) as explained bellows. We refer to this list as L_1-list which is initially empty. When F makes a H_1-query with ID, the algorithm B responses as follows:

- If the query ID already appear on the L_1-list in a tuple (ID, b, c), then it responds with $H_1(ID) = \omega$
- Otherwise, B chooses a random coin $c \in \{0, 1\}$ with

$$Pr[c = 0] = \frac{1}{q_e + 1}$$

If c = 0, then B randomly picks $b \in Z_q$ to compute w = byP. If c = 1, then B randomly picks $b \in Z_q$ to compute w = bP.

Finally, B records the tuple (ID, w, b, c) in the L_1-list and responds to F with $w = H_1(ID)$.

H_2-oracles: when F makes hash queries on H_2-oracle with (U, a, m) B searches the pair (ω, U, a, m) in the list L2 which maintains the tuples (ω, U, a, m), if such a pair exists, then B responses ω to F, otherwise, B randomly chooses $\omega \in Z_q$ to answer F and records this pair (ω, U, a, m) in the list L_2.

H_3-oracles: When F makes queries on H_3-oracle with t, B searches the pair (a, t) in the list L_3 which maintains the tuples (a, t) if such a pair exists, B responses α to F. Otherwise, B randomly chooses $a \in G_2$ to answer F and records this pair (t, a) in the list L_3.

Extract queries: When F queries the private key corresponding to ID, B searches the corresponding tuple (ID, w, b, c) in the L_1-list.

- If c=0, then B fails and aborts it
- Otherwise, B computes $s_{ID} = bP^1_{pub}$ and responds to F with s_{ID} as a private key of ID

Signcryption Querie: When F makes a signcryption query on message m with L = (ID_A, ID_B), B searches the corresponding tuples (ID_A, w_A, b_A, c_A) in the L_1-list:

- If ID_A exists in the L_1-list, it means that was previously queried. Thus, B is able to compute signcryption of message m by using the above Signcrypt algorithm
- Otherwise, B fails and aborts it

If B does abort as a result of F's Extract queries and Signcryption queries, then F's view is identical to its view in the real attack.

Output: Eventually, A outputs a forgery $\delta^* = (U^*, W^*)$ on a message m^*. By adopting the forking lemma, we use the same tape, then we will obtain the other pair signature $\delta^{1*} = (U^{1*}, W^{1*})$ on the same message m^*. By previous assumption, ID^*_A and message m^* must been queried to H_1-oracle. If the coin flipped by B for the query with the identity, which did not show 0 then B declares "failure". Otherwise, if the coin flipped c^*_m=1 by B for message m^*, then B aborts it, if $c^*_m = 0$ (it means that $H_1(m^*) = b^*_m P$) and B has the master secret key of PKG_2, it means that B has the secret key of the recipient, he can response as follows:

Without loss of generality, ID^*_i is the honest signer, thenc*1. We have:

$$V^* = r^* P^1_{pub} + hS_A$$
$$V'^* = r'^* P^1_{pub} + h'S_A$$

It means that B is able to the instance of the CDH problem:

$$xyP = \frac{1}{h - h'}(V^* - V'^*)$$

CONCLUSION

Signcryption is a relatively new cryptographic technique that is supposed to fulfill the functionalities of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes. By combining two ID-based signature schemes with ID-based signcryption scheme, we build security model of signcryption in the multi-PKG and based on the bilinear pairings to adapt to multi-PKG cryptgraphical systeme setting. The scheme can be applied in multiple autonomous domain environments such as decentralized self-organization network, autonomous P2P and large scale distributed trust management environment etc. At the same time, we also prove that our proposed scheme is secure and satisfies the confidentiality and unforgeability. It remains an open problem to design identity-based signcryption scheme that is secure in the standard model.

ACKNOWLEDGMENTS

I thank the anonymous referees for their very valuable comments on this study. This work is supported by, the New Star Plan Project of Beijing Science and Technology (No: 2007B-001)and and The Beijing Natural Science Foundation Programm and Scientific Research Key Program of BeijingMunicipal Commission of Education (No: KZ2008 10009005).

REFERENCES

Baek, J., R. Steinfeld and Y. Zheng, 2002. Formal proofs for the security of signcryption. Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography, (IWPTPKC'02), Springer-Verlag, London, pp: 80-98.

Barreto, P.S., B. Libert, N. McCullagh and J. Quisquater, 2005. Efficient and provably-secure identity-based signatures and signcrypion from bilinear maps. Proceedings of the Asiacrypt, LNCS 3788, (ALNCS'05), Springer-Verlag, pp: 515-532.

Boyen, X., 2003. Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. Proceeding of the Advances in Cryptology, LNCS 2729, (ACL'03), Springler-Verlag, pp: 383-399.

Chow, S.S.M., S.M. Yiu, L.C.K. Hui and K.P. Chow, 2004. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. Porceeding of the Information Security and Cryptology, LNCS 2971, (ICISC'03), Springer-verlag, pp: 352-369.

Libert, B. and J. Quisquater, 2003. A new identity based signcryption schemes from pairings. Poceedings of the IEEE Information Therory Workshop, 31 March-4 April, IEEE, pp: 155-158.

Libert, B. and J.J. Quisquater, 2004. Efficient signcryption with key privacy from gap diffie-hellman groups. Proceedings of the Public Key Cryptography, (PKC'04), Springer-Verlag, pp: 187-200.

Malone-Lee, J., 2002. Identity based signcrption. Cryptology ePrint Archive, Report 2002/098. http://eprint.iacr.org/2002/098

Tan, C.H., 2005. On the security of signcryption scheme with key privacy. IEICE Trans. Fundam., E88-A: 1093-1095.

Wang, X. and H. Qian, 2010. Attacks against two identity-based signcryption schemes. Porceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing, April 24-25, Wuhan, Hubei, pp: 24-28.

Zhang, M., B. Yang, S. Zhu and W. Zhang, 2008. Assertions signcryption scheme in decentralized autonomous trust environments. Proceedings of the 5th International Conference on Autonomic and Trusted Computing, (ICATC'08), Springer-Verlag, pp: 516-526.

Zheng, Y., 1997. Digital signcryption or how to achieve cost (signature and encryption)« cost (signature) + cost (encryption). Proceedings of the 17th Annual International Cryptology Conference Santa Barbara, California, USA., LNCS 1294, Aug. 17-21, Springer-Verlag, Berlin, pp: 165-179.