A Computational Review of Identity-based Signcryption Schemes

Murari Mandal[1], Gaurav Sharma[2], and Anil K. Verma[1]
(Corresponding author: Gaurav Sharma)
Computer Science and Engineering Department, Thapar University, Patiala-147004, India[1]
Amity School of Engineering, Amity University, Noida, India[2]
(Email: sharmagaurav86317@gmail.com)
(Received Jan. 20, 2015; revised and accepted July 4 & Dec. 7, 2015)

Abstract

Since 2002, several identity based signcryption schemes have been proposed. The purpose of designing a signcryption scheme is to perform signature and encryption both in one step but at lesser cost than performing signature and then encryption separately. In this paper, we present a literature survey on signcryption schemes for identity based setup. Our primary focus is on the schemes recently developed in standard model as the schemes in random oracle model are not actually practical. We present detailed comparison among the schemes based on computation cost, security features and suggest some final recommendation based on some future perspectives.

Keywords: Identity based cryptography, public key cryptography, signcryption, standard model

1 Introduction

The field of cryptography deals with providing various aspects of security for computer based communication [37]. For network based communications, confidentiality and authentication are the two most essential security features, which must be addressed. Confidentiality of message communicated between two or more users can be achieved through encryption. The properties of authentication (to confirm/verify the sender's identity), integrity (the message should not get altered before reaching the receiver) and non-repudiation (the sender can not deny the authorship of the message after the completion of the communication) are achieved by signatures.

The concept of identity based cryptography was first introduced by Shamir [33] in 1984. In ID based encryption/signature schemes, the identity of the user is used as the public key, or some well-known algorithms (or hash functions) are used to derive the same. Such an identity can be the email address, social security number or some string that can help to identify the user unambiguously. This alleviates the certificate management issue as the public key is implicitly authenticated. Although, the necessity of PKI (Public Key Infrastructure) is removed but this does require a PKG (Private Key Generator), which acts as a trusted authority to generate the private keys for the user with respect to their identity as and when requested by the user.

The implementation of ID Based Signature scheme (IBS) were presented by [13, 16] but, until 2001 the practical implementation of IBE (ID Based Encryption) was an open problem. Boneh and Franklin [7] presented the first practical IBE using bilinear pairing over elliptic curves.

Many other IBE schemes [6, 31, 34, 39] were proposed thereafter. In ID based encryption/signature schemes, some other security properties are also introduced such as public verifiability, forward secrecy etc. We will discuss about these terms in the later sections of this paper.

In 1997, Zheng [41] coined a term signcryption, which he derived by combining the words signature and encryption. The idea was to achieve signature and encryption both in a single logical step (in a single algorithm), which will cost less than the combined cost of performing signature and then encryption with the help of two separate algorithms. Zheng also presented a signcryption scheme based on Discrete Logarithm Problem (DLP).

Later, Baek et al. [9] presented the security proof for Zheng's scheme by introducing a security model. In 2002,

Malone-Lee [28] proposed the first identity based signcryption scheme including its security model. Later on, many signcryption schemes [4, 8, 11, 12, 27, 29] were presented. Most of these schemes were proven secure in the random oracle model by Bellare and Rogaway [5]. Although, the schemes provably secure in the random oracle model are quite efficient but the flaw in this model were pointed out in [2, 3, 10, 15]. Yu et al. [40] proposed the first identity based signcryption scheme without random oracle. Their scheme is based on Water's scheme [39]. Thereafter, several signcryption schemes were proposed in standard model. A survey of identity based signcryption was carried out by Li and Khan [22] by analysing ten signcryption schemes and their security parameters.

Since, the paper did not discuss much about the comparison among the signcryption schemes in standard model (only two schemes) as very few paper were published till that time. In this paper, we present a detailed analysis of the signcryption schemes and compare their efficiency and security properties.

The rest of the article is organized as follows. Section 2 contains preliminaries about the bilinear pairings. In Section 2.3, we give a general setup for signcryption scheme. In Section 3 we describe several security models. In Section 4 we give detailed analysis of the various signcryption schemes both in random oracle model and in standard model with help of the tables and in Section 5 we conclude our paper with some suggestions for future work.

2 Preliminaries

This section describes bilinear pairings and computational hardness problems, which are taken into consideration for the designing of an ID based signcryption schemes.

2.1 Bilinear Pairings

Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_T$ be a multiplicative group of prime order p. Then, bilinear pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$, which satisfies the following conditions:

- *Bilinearity*: For all $X, Y, Z \in \mathbb{G}_1$, $\hat{e}(X + Y, Z) = \hat{e}(X, Z) \cdot \hat{e}(Y, Z)$ and $\hat{e}(X, Y + Z) = \hat{e}(X, Y) \cdot \hat{e}(X, Z)$;
- *Non-degeneracy*: $\hat{e}(X, X) \neq 1$;
- *Computability*: $\forall X, Y \in \mathbb{G}_1$, there is an efficient algorithm to compute $\hat{e}(X, Y)$.

Many pairing based cryptographic schemes use the bilinear pairing and depend on the intractability of some known problem like BDHP (Bilinear Diffie-hellman Problem), DBDHP (Decisional Bilinear Diffie-hellman Problem), CBDHP (Computational Bilinear Diffie-hellman Problem), etc.

2.2 Computational Hardness Problems

This section provides the computational hardness problems, which are used as a base to the security protocols.

Definition 1. Computational Diffie-Hellman Problem (CDHP)*: Given a generator P of $\mathbb{G}$ and aP, bP for unknown $a, b \in_R \mathbb{Z}_n^*$, the task of CDHP is to compute abP.*

Definition 2. Decisional Diffie-Hellman Problem (DDHP)*: Given a generator P of $\mathbb{G}$ and aP, bP, cP for unknown $a, b, c \in_R \mathbb{Z}_n^*$ the task of DDHP is to decide whether the equation $abP = cP$ holds.*

Definition 3. Gap Diffie-Hellman Problem (GDHP)*: Given a generator P of $\mathbb{G}$ and aP, bP for unknown $a, b \in_R \mathbb{Z}_n^*$ and an oracle DDHP (aP, bP, cP), which returns 1 if and only if $abP = cP$, the task of GDHP is to compute abP. The Gap Diffie-Hellman Assumption (GDHA) states that the probability of any polynomial-time algorithm solving the GDHP is negligible.*

2.3 General Setup

Lee [28] proposed the first IDSC (Identity Based Signcryption Scheme). We derive our general setup for IDSC from that scheme. The general setup for signcryption is explained in Table 1 and the process of secure exchange of message between the sender and receiver with the help of PKG is diagrammatically presented in Figure 1.

3 Security Models

Although, confidentiality and unforgeability are the two primary security requirements for any signcryption schemes but there are some special security properties like forward secrecy and public verifiability that have become essential for IDSC. In addition to this, Boyen [8] and Chow et al. [12] have defined few more security features like ciphertext unlinkability, ciphertext authentication, ciphertext anonymity and public ciphertext verifiability (see Figure 2). A single signcryption algorithm may not be able to ensure all these additional security features, as we will see that some of them contradict with each other. But, having some of these specialized security parameters might be very effective for security in a particular domain. We will discuss these security parameters in view of identity based signcryption setup. In the rest of this section we will give generalized definition of all the security parameters that we have mentioned above. Since every author defines his own security model based on which he gives his security results, our purpose is to give our readers a general idea about these security models.

3.1 Confidentiality

Confidentiality ensures that any third party (except the sender and receiver) will not be able to access or derive any information about the message being communicated. An et al. [1] suggested the notion of insider security and outsider security models. In the outsider security model, the adversary only has access to his own private key and he can signcrypt the message using the public keys of other users i.e. the adversary is having capability just like a user. Since, this is very weak assumption about an adversary so, we will neglect this case in the rest of our paper. In the insider security model, an adversary is given the power to perform adaptive chosen ciphertext attack also known as CCA2. It gives an access to adversary to unsigncrypt oracle, so that, he can unsigncrypt any ciphertext of his own choice (of course except the challenge ciphertext, otherwise life would be so easy for him, right!). In the rest of our paper we will only consider the insider security model.

Table 1: General setup for signcryption

Step	Action Performed
Setup	• For a given input 1^k, the PKG generates system parameters using some algorithm, where k is some security parameter • It also generates master public key mst_p and master private key mst_s. It keeps the master private key secret to himself
Extract	• For a given input (identity of the user), the PKG uses Extract algorithm to generate the private key and gives it to the user • The Extract algorithm will make use of the master private key mst_s for this purpose e.g. if user A with identity ID_A requests for a private key then, the private key $S_{ID_A} = Extract(ID_A)$
Signcrypt	• If ID_A wants to send a message m to ID_B, then the Signcrypt algorithm takes as input the message m, the private key of the sender ID_A and the identity of the receiver ID_B. The output ciphertext $\sigma = Signcrypt(m, S_{ID_A}, S_{ID_B})$
Unsigncrypt	• This algorithm takes the ciphertext σ as input, the identity of the sender ID_A and the private key of the receiver S_{ID_B} and returns a message m or symbol $\perp$ if the ciphertext is invalid one • Consistency check: If $\sigma = Signcrypt(m, S_{ID_A}, ID_B)$, then $m = Unsigncrypt(\sigma, S_{ID_B}, ID_A)$

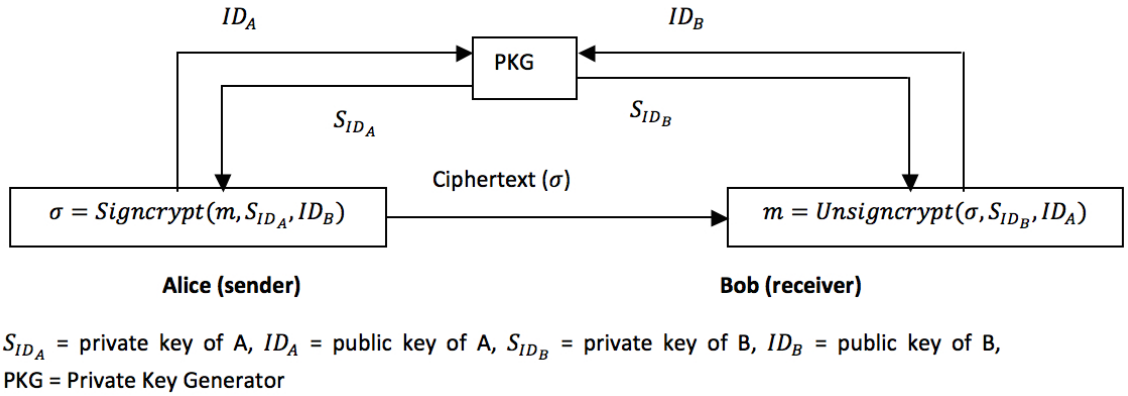

Figure 1: ID based signcryption

The following game is played between the challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

1) $\mathcal{C}$ runs the setup algorithm with security parameter k and gives the system parameters to the Probabilistic Polynomial Time (PPT) adversary $\mathcal{A}$.

2) **Phase 1:** $\mathcal{A}$ makes a polynomially bounded number of queries adaptively. By the term "Adaptively", we mean that every request can depend on the response to the previous query.

   a. *Key Extraction*: $\mathcal{A}$ gives an identity ID_A and $\mathcal{C}$ computes $S_{ID_A} = Extract(ID_A)$ and gives S_{ID_A} to $\mathcal{A}$.

   b. *Signcryption Queries*: $\mathcal{A}$ requests the challenger $\mathcal{C}$ to produce a signcryption on the message m by the sender ID_A to the receiver ID_B. Challenger responds with private key S_{ID_A} and $\sigma = Signcrypt(m, S_{ID_A}, ID_B)$.

   c. *Unsigncrypt Queries*: $\mathcal{A}$ requests to unsigncrypt a ciphertext σ with sender's identity ID_A and the receiver's identity ID_B to the challenger $\mathcal{C}$. The challenger responds with results as follows:

      i. The private key of ID_B. $S_{ID_B} = Extract(ID_B)$.

      ii. $UnSigncrypt(\sigma, S_{ID_B}, ID_A)$, the result can be the symbol $\perp$ in case of invalid ciphertext as input.

3) The adversary can make as many queries as he wants in the *Phase 1*, with restriction that he can't ask for the private key of the receiver of the actual ciphertext on which he is being challenged.

   a. The adversary chooses two plaintexts m_0, m_1 and the sender's identity ID_S and the receiver's identity ID_R on which he wants to be challenged. Remember that he can't make extraction query on ID_R in *Phase 1*.

   b. The challenger takes a random bit $b \in \{0,1\}$ and computes $\sigma^* = Signcrypt(m_b, S_{ID_S}, ID_R)$ and gives σ^* to $\mathcal{A}$.

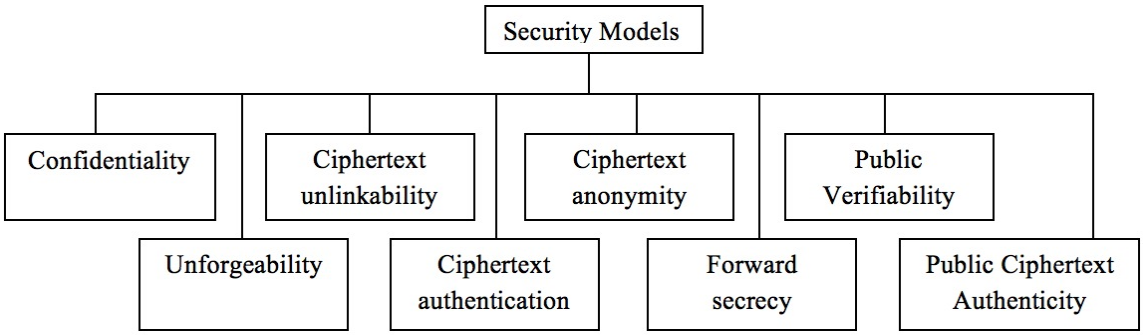

Figure 2: Security models

4) **Phase 2:** $\mathcal{A}$ can perform a polynomially bounded number of queries adaptively, similar to *Phase 1* but with restriction that he can't make key extraction query on ID_R or ID_S. Also, he can't make an unsigncrypt query on σ^*. $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$. The advantage of $\mathcal{A}$ is defined as $Adv(\mathcal{A}) = |Probability(b' = b) - \frac{1}{2}|$.

Definition 4. *An ID based signcryption scheme IDSC is IND-CCA2 (Indistinguisability against adaptively Chosen Ciphertext Attack) secure if a PPT adversary $\mathcal{A}$ doesn't have non-negligible advantage in the above game.*

3.2 Unforgeability

This property ensures that the adversary can't produce the similar signature as of the challenger on a given message. For IDSC we consider the following game played between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. The Steps 1 to 4 of previous section will be again repeated for this game. So, we will directly discuss the 5th step. $\mathcal{A}$ generates a new triple (σ^*, ID'_S, ID'_R) i.e. a triple, which was not generated by the signcryption oracle. The adversary $\mathcal{A}$ was not allowed to make request for the private key of ID'_S during the *Phase 1* of the game. At the same time the adversary is allowed to request for the private key of the receiver, this will prevent a dishonest receiver to make forgery of the sender.

$\mathcal{A}$ wins the game if $UnSigncrypt(\sigma^*, S_{ID'_R}, ID'_S) \neq \perp$.

Definition 5. *An IDSC scheme is EU-CMA (Existential Unforgeability against Chosen Message Attack) secure if for all PPT adversaries, the advantage of $\mathcal{A}$ in the above game i.e. $Adv(\mathcal{A})$ = Probability of success in above game is negligible.*

3.3 Ciphertext Unlinkability

This property gives the sender of a message the power to deny having sent a message to the receiver even if that message might contain the signature of the sender only. It means that although the message is signed by the sender only but whether the ciphertext was sent by the sender or not can't be verified by anyone. Such property may be very helpful in certain situations such as security agents communicating with their base station from and some other cases as mentioned by Boyen [8].

3.4 Ciphertext Authentication

This property is kind of an exception case of Ciphertext Unlinkability. The receiver can authenticate that the ciphertext indeed came from the sender who has signed the message that it contains but he can't prove it to anyone. The detailed description is given by Boyen [8].

3.5 Ciphertext Anonymity

This property makes the ciphertext anonymous i.e. except the receiver no one should be able to know about the author or recipients of the message.

3.6 Forward Secrecy

Forward secrecy means that even if a private key of the sender gets compromised, still it will not be possible for someone to unsigncrypt the messages that were signcrypted previously by the user [12]. In the insider security model, forward secrecy is naturally achieved because if a scheme is CCA2 secure then it will also provide forward secrecy.

3.7 Public Verifiability

This property states that if a ciphertext is provided by the receiver and also the corresponding message and some other information to a trusted third party, the third party should be able to verify that the ciphertext is valid signature on the message by the sender even if the private key of the sender is not available.

3.8 Public Ciphertext Authenticity

This notion was presented by Chow et al. [12]. This property makes it possible for any third party to verify the ciphertext's origin and also to check its validity. The third

party is not allowed to get any information from the receiver. This property directly contradicts with the ciphertext authenticity definition above, so it is not possible to achieve both of them simultaneously in one scheme.

4 Analysis of Identity Based Signcryption Schemes

We divide our discussion in two parts. First we will discuss about the schemes that are proposed under random oracle model and then about the schemes proposed in standard model.

4.1 Identity Based Signcryption Schemes in Random Oracle Model

After the practical implementation of ID based encryption by Boneh and Franklin [7], Malone-Lee [28] proposed the first ID based signcryption scheme. He also presented a security model to prove its security. But, Libert and Quisquater [27] pointed out that since the signature on the plaintext is visible in the ciphertext, therefore the scheme can not ensure confidentiality of the message. They proposed three new schemes, the first one alleviated the semantic security issue, in the second scheme they modified the previous scheme to produce shorter ciphertext and in the last scheme they added the forward secrecy property but by doing this the scheme lost the public verifiability property. They further proposed an open problem to construct a signcryption scheme that provides both forward secrecy and public verifiability. In 2004, this problem was solved by Chow et al. [12]. They not only designed a new scheme that provides both forward secrecy and public verifiability but also added a new security property called public ciphertext authenticity. In the same year McCullagh and Barreto [29] also presented a new scheme to address the same issue.

In 2003, Boyen [8] introduced some specialized security parameters, such as, ciphertext unlinkability, ciphertext authentication, ciphertext anonymity and presented a scheme to achieve a two layer sign and then encrypt combination. This scheme facilitates multi-recipient signcryption i.e. encrypting the same message with a shared signature and also single bulk message encryption. In 2005, Chen and Malone-Lee [11] improved Boyen's [8] scheme and made it more efficient. Barreto et al. [4] improved it further to achieve the most efficient ID based signcryption scheme. In 2007, Li et al. [21] presented an efficient signcryption scheme with the property of ciphertext anonymity.

Since, security proof in random oracle models are not applicable in real time situations [2, 3, 10, 15], therefore it is important to design schemes that are secure in standard model. In the next section we discuss about such schemes.

4.2 Identity Based Signcryption Schemes in Standard Model

In 2009, Yu et al. [40] proposed the first ID based signcryption scheme in the standard model. They combined the ideas from Waters [39] and Paterson and Schuldt's [32] to design their new scheme. This scheme was proved insecure by Bo Zhang [42], Zhengping et al. [17], Wang and Qian [38] and Zhang et al. [43]. This scheme is vulnerable to IND-CCA2 attack and the SUF-CMA attack and therefore this scheme is neither semantically secure nor unforgeable. The improved scheme proposed by Zhengping et al. [17] was also cryptanalysed by Li et al. [14]. In 2010, Zhang [42] proposed a scheme, which was later proved IND-CCA2 insecure by Li and Takagi [24], thus attacking the semantic security of this scheme but it still provides unforgeability. Li and Takagi [24] improved Zhang's [42] scheme and proposed a new scheme, which was proven both IND-CCA2 and EUF-CMA insecure by Selvi et al. [35]. Further improvement given by Li et al. [25] was also proven insecure by Selvi et al. [35]. In 2011, another scheme was proposed by Li et al. [23] in which they achieved both confidentiality and unforgeability at less computational cost in comparison to previous schemes. But flaws in their proof for security against IND-CCA2 attack were pointed out by Selvi et al. [35]. Selvi et al. [35] presented a signcryption scheme by direct combination of IBE and IBS. They took the IBS in standard model proposed by Paterson and Schuldt [32] and IBE in standard model proposed by Kiltz and Vahlis [18]. They followed sign and then encrypt method as this is the only combination that is both IND-CCA2 and EUF-CMA secure. Although this scheme is secure but it does suffer from inefficiency.

In 2012, Li et al. [26] presented a fully secure ID based signcryption scheme, which is having shorter ciphertext than the previous schemes. They also compared the efficiency of their scheme with previous schemes and presented an analysis based on that. Such a scheme may be preferable in real time applications. But later, Ming and Wang [30] proved that their scheme is not semantically secure against chosen-message attacks and it is also not existentially unforgeable against chosen-message attacks. Lee et al. [20] presented a signcryption scheme that produced even shorter ciphertext in size compared to Li et al.'s scheme. Kushwah and Lal [19] present two ID based signcryption schemes, the first one provides the semantic security and unforgeability and the second scheme provides public ciphertext authentication. In 2012, Selvi et al. [36] proposed the most secure ID based signcryption scheme in standard model. Their security model fulfills the strongest notion for security in identity based signcryption schemes. Their scheme provides public ciphertext authenticity. But this increased the computational cost for the scheme. So, we can see that there is trade-off between the tightness of security and the efficiency of any signcryption scheme.

The computational costs of all the signcryption

schemes that have been discussed are tabulated in Table 2. In Table 2, in the pairing (Pair) column we have considered the total number of pairings required to either signcrypt or unsigncrypt. Multiplications (Mul), Exponentiations (Exp), Inverse (Inv), Addition/Subtraction (Add/Sub) are all performed in group (either in $\mathbb{G}_1$ or in $\mathbb{G}_T$). All these constitute to the cost of computation of a signcryption scheme. In the Hash column, only the number of hashing performed is listed and the type of hash function depends on the choice of the designer. ID_L denotes the bit length of all the identities and M_L denotes the bit length of the message. In a row, for example in the first row, the upper row describes the computational cost for signcryption and the lower row describes the cost in unsigncryption. ROM refers to "Random Oracle Model" and SM to "Standard Model".

The security analysis is presented in Table 3. The Cryptanalysis (C.A.) column describes by which author the cryptanalysis was done and the Attack (Att.) column describes which type of attack was made. The security parameters considered are Confidentiality (Con), Unforgeability (Unf), Public Verifiability (PuV), Forward Secrecy (FoS), Ciphertext Unlinkability (CiU), Ciphertext Anonymity (CiA), Ciphertext Authenticity (CiAu), Public Ciphertext Authenticity (PuCA).

5 Conclusion

Identity based signcryption has become a very important area of research as it performs both encryption and signature in one logic step and at lesser cost than direct combination of signature and encryption. By this survey we draw following conclusions:

1) Since random oracle models are not feasible to implement in real time applications, so schemes in standard model with tighter security and more efficiency, need to be designed.

2) The cost efficiency of signcryption can be very useful in areas such as wireless sensor networks, mobile ad hoc networks. Further new areas of implementation of ID based signcryption need to be explored.

3) The security of the latest IDSC schemes also has to be analysed. Since, most of the previous schemes in standard model has been cryptanalysed so it is important to thoroughly analyze the latest schemes before implementing them for practical purpose.

References

[1] J. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Advances in Cryptology (Eurocrypt'02)*, LNCS 2332, pp. 83–107, Springer, 2002.

[2] B. Barak, "How to go beyond the black-box simulation barrier," in *Proceedings of 42nd IEEE Symposium on Foundations of Computer Science*, pp. 106–115, 2001.

[3] B. Barak, Y. Lindell, and S. Vadhan, "Lower bounds for non-black-box zero knowledge," in *Proceedings of 44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 384–393, 2003.

[4] P. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology (Asiacrypt'05)*, LNCS 3788, pp. 515–532, Springer, 2005.

[5] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62–73, 1993.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pp. 417–42, 2008.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal of Computing*, vol. 32, pp. 586–615, 2003.

[8] X. Boyen. "Multipurpose identity-based signcryption," in *Advances in Cryptology (Crypto'03)*, LNCS 2729, pp. 383–399, Springer, 2003.

[9] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," in *Public Key Cryptography*, LNCS 2274, pp. 80–98, Springer, 2002.

[10] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, pp. 557–594, July 2004.

[11] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography (Pkc'05)*, LNCS 3386, pp. 362–379, Springer, 2005.

[12] S. Chow, S. Yiu, L. Hui, and K. 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'03)*, LNCS 2971, pp. 352–369, Springer, 2004.

[13] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology (Crypto'86)*, LNCS 263, pp. 186–194, Springer, 1987.

[14] L. Fagen, Q. Zhiguang, "Analysis of an identity-based signcryption scheme in the standard model," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 94, no. 1, pp. 268–269, 2011.

[15] S. Goldwasser and Y. Kalai, "On the (in)security of the fiat-shamir paradigm," in *Proceedings of 44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 102–113, 2003.

[16] L. Guillou and J. Quisquater, "A "paradoxical" indentity-based signature scheme resulting

Table 2: Computational cost comparison

IDSC	Pair	Exp	Mul	Hash	Inv	Add/Sub	Model
Malone-Lee [28]	1	0	3	3	0	1	ROM
	4	1	0	2	0	0	
Libert and Quisquater* [27]	2	2	2	3	0	1	ROM
	4	2	2	3	0	0	
Libert and Quisquater* [27]	2	2	2	4	0	1	ROM
	4	2	2	4	1	0	
Libert and Quisquater* [27]	1	1	3	3	0	1	ROM
	2	0	2	3	0	0	
Boyen [8]	1	4	3	6	0	0	ROM
	4	2	1	7	0	0	
Chow et al.* [12]	2	0	2	2	0	0	ROM
	4	0	3	2	0	0	
Chen and Malone-Lee [11]	1	0	3	4	0	0	ROM
	3	0	1	4	0	0	
Barreto et al. [4]	0	1	3	3	0	1	ROM
	2	1	2	3	1	1	
McCullagh et al. [29]	0	1	2	2	0	0	ROM
	2	1	1	2	0	0	
McCullagh et al. [29]	0	1	3	2	0	0	ROM
	2	0	1	2	0	1	
Li et al. [21]	0	0	3	2	0	0	ROM
	4	0	1	2	0	0	
Yu et al.[40]	1	4	$ID_L + M_L + 2$	1	0	0	SM
	6	0	$ID_L + M_L + 4$	1	1	0	
Zhengping et al. [17]	1	4	$ID_L + M_L + 2$	1	0	0	SM
	6	0	$ID_L + M_L + 4$	1	1	0	
Zhang [42]	1	6	$ID_L + M_L + 3$	2	0	0	SM
	6	2	$ID_L + M_L + 5$	2	2	0	
Li and Takagi [24]	1	6	$2ID_L + M_L + 3$	2	0	0	SM
	6	2	$ID_L + M_L + 5$	2	1	0	
Li et al.* [25]	0	6	$ID_L + M_L + 1$	1	0	0	SM
	5	0	$ID_L + M_L + 3$	0	1	0	
Li et al. [26]	1	4	$ID_L + M_L + 2$	1	0	0	SM
	6	0	$ID_L + M_L + 4$	1	1	0	
Selvi et al. [36]	1	5	$ID_L + M_L + 3$	4	0	0	SM
	6	2	$ID_L + M_L + 5$	4	1	0	
Selvi et al.* [35]	1	8	$ID_L + M_L + 3$	2	0	0	SM
	6	3	$ID_L + M_L + 5$	1	0	0	
Li et al.* [23]	0	5	$ID_L + M_L + 3$	2	0	0	SM
	5	2	$ID_L + M_L + 6$	2	1	0	
Lee et al. [20]	0	7	$ID_L + M_L + 3$	4	0	0	SM
	4	2	$ID_L + M_L + 5$	3	1	0	
Kushwah and Lal [19]	1	4	$2ID_L + M_L + 1$	3	0	0	SM
	6	0	$ID_L + M_L + 3$	2	2	0	
Kushwah and Lal [19]	1	4	$ID_L + M_L + 2$	2	0	0	SM
	6	0	$ID_L + M_L + 4$	2	1	0	

* This scheme also uses a symmetric cipher.

Table 3: Security analysis

IDSC	Con	Unf	PuV	Fos	CiU	CiAn	CiAu	PuCA	C.A.	Att.
Malone-Lee [28]	N	Y	Y	Y	N	N	N	N	[27]!	1
Libert and Quisquater* [27]	Y	Y	Y	N	N	N	N	N		
Libert and Quisquater* [27]	Y	Y	Y	N	N	N	N	N		
Libert and Quisquater* [27]	Y	Y	N	Y	N	N	N	N		
Boyen [8]	Y	Y	Y	Y	Y	Y	Y	N		
Chow et al.* [12]	Y	Y	Y	Y	N	N	N	Y		
Chen and Malone-Lee [11]	Y	Y	Y	Y	Y	Y	Y	N		
Barreto et al. [4]	Y	Y	Y	Y	N	N	N	N		
McCullagh et al. [29]	Y	Y	N	Y	N	N	N	N		
McCullagh et al. [29]	Y	Y	Y	Y	N	N	N	N		
Li et al. [21]	Y	Y	Y	Y	N	Y	N	N		
Yu et al.[40]	N	N	Y	Y	N	N	N	N	[38, 42, 43, 17]	3, 4
Zhengping et al. [17]	N	N	Y	Y	N	N	N	N	[14]	1, 2
Zhang [42]	N	Y	Y	Y	N	N	N	N	[24]	1
Li and Takagi [24]	N	N	Y	Y	N	N	N	N	[35]	1, 2
Li et al.* [25]	N	N	Y	Y	N	N	N	N	[35]	1, 2
Li et al. [26]	Y	Y	Y	Y	N	N	N	N	[30]	1, 2
Selvi et al. [36]	Y	Y	Y	Y	N	N	Y	N		
Selvi et al.* [35]	Y	Y	Y	Y	N	N	N	Y		
Li et al.* [23]	Y#	Y	Y	Y	N	N	N	N	[35]	
Lee et al. [20]	Y	Y	Y	Y	N	N	N	N		
Kushwah and Lal [19]	Y	Y	N	Y	N	N	N	N		
Kushwah and Lal [19]	Y	Y	Y	Y	N	N	N	Y		

! Security weakness in semantic security was pointed out. # Flaw in the security proof as pointed out by [35]. 1→IND-CCA2, 2→EUF-CMA, 3→IND-IDSC-CCA [40], 4→EUF-IDSC-CMA [40].

from zero-knowledge," in *Advances in Cryptology (Crypto'88)*, LNCS 403, pp. 216–231, Springer, 1990.

[17] Z. Jin, Q. Wen, H. Du, "An improved semantically-secure identity-based signcryption scheme in the standard model," *Computers & Electrical Engineering*, vol. 36, no. 3, pp. 545–552, 2010.

[18] E. Kiltz and Y. Vahlis, "CCA2 secure IBE: Standard model efficiency through authenticated symmetric encryption," in *Topics in Cryptology (Ctrsa'08)*, LNCS 4964, pp. 221–238, Springer, 2008.

[19] P. Kushwah and S. Lal, "Provable secure identity based signcryption scheme without random oracles," *International Journal of Network Security & Its Applications*, vol. 4, no. 3, pp. 97 – 110, 2012.

[20] P. Lee, P. Udaya, and N. Shivaramakrishnan, "Efficient identity-based signcryption without random oracles," in *Proceedings of the Tenth Australasian Information Security Conference*, vol. 125, 2012.

[21] C. Li, G. Yang, D. Wong, X. Deng, and S. Chow, "An efficient signcryption scheme with key privacy," in *Public Key Infrastructure*, LNCS 4582 of, pp. 78–93, Springer, 2007.

[22] F. Li and M. Khan, "A survey of identity-based signcryption," *IETE Technical Review*, vol. 28, no. 3, pp. 265–272, 2011.

[23] F. Li, F. Muhaya, M. Zhang, and T. Takagi, "Efficient identity-based signcryption in the standard model," in *Provable Security*, LNCS 6980, pp. 120–137, Springer, 2011.

[24] F. Li and T. Takagi, "Secure identity-based signcryption in the standard model," *Mathematical and Computer Modelling*, vol. 57, no. 11C12, pp. 2685–2694, 2013.

[25] F. Li, L. Yongjian, Q. Zhiguang, and T. Takagi, "Further improvement of an identity-based signcryption scheme in the standard model," *Computers & Electrical Engineering*, vol. 38, no. 2, pp. 413–421, 2012.

[26] X. Li, H. Qian, J. Weng, and Y. Yu, "Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model," *Mathematical and Computer Modelling*, vol. 57, no. 3C4, pp. 503 – 511, 2013.

[27] B. Libert and J. Quisquater, "New identity based signcryption schemes from pairings," IACR Cryptology ePrint Archive, Report 2003/023, 2003.

[28] J. Malone-Lee, "Identity-based signcryption," IACR Cryptology ePrint Archive, Report 2002/098, 2002.

[29] N. McCullagh and P. Barreto, "Efficient and forward-secure identity-based signcryption," IACR Cryptology ePrint Archive, Report 2004/117, 2004.

[30] Y. Ming and Y. Wang, "Cryptanalysis of an identity based signcryption scheme in the standard model," *International Journal of Network Security & Its Applications*, vol. 18, no. 1, pp. 165–171, 2016.

[31] D. Naccache, "Secure and practical identity-based encryption," *IET Information Security*, vol. 1, no. 2, pp. 59–64, 2007.

[32] K. Paterson and J. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Information Security and Privacy*, LNCS 4058, pp. 207–222, Springer, 2006.

[33] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, LNCS 196, pp. 47–53, Springer,1985.

[34] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology (Eurocrypt'05)*, LNCS 3494, pp. 457–473, Springer, 2005.

[35] S. Selvi, S. Vivek, D. Vinayagamurthy, and C. Rangan, "On the security of id based signcryption schemes," IACR Cryptology ePrint Archive, Report 2011/664, 2011.

[36] S. Selvi, S. Vivek, D. Vinayagamurthy, and P. Rangan, "ID based signcryption scheme in standard model," in *Provable Security*, Lecture Notes in Computer Science, pp. 35–52, Springer Berlin Heidelberg, 2012.

[37] G. Sharma, S. Bala, and A. K. Verma, "An improved RSA-based certificateless signature scheme for wireless sensor networks," vol. 18, no. 1, pp. 82–89, 2016.

[38] X. Wang and H. Qian, "Attacks against two identity-based signcryption schemes," in *IEEE Second International Conference on Networks Security Wireless Communications and Trusted Computing*, vol. 1, pp. 24–27, 2010.

[39] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology (Eurocrypt'05)*, LNCS 3494, pp. 114–127, Springer, 2005.

[40] Y. Yu, B. Yang, Y. Sun, and S. Zhu, "Identity based signcryption scheme without random oracles," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 56–62, 2009.

[41] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost (encryption)," in *Advances in Cryptology (Crypto'97)*, LNCS 1294, pp. 165–179, Springer, 1997.

[42] B. Zhang, "Cryptanalysis of an identity based signcryption scheme without random oracles," *Journal of Computational Information Systems*, vol. 6, no. 6, pp. 1923–1931, 2010.

[43] M. Zhang, P. Li, B. Yang, H. Wang, and T. Takagi, "Towards confidentiality of ID-based signcryption schemes under without random oracle model," in *Intelligence and Security Informatics*, LNCS 6122, pp. 98–104, Springer, 2010.

Anil Kumar Verma is currently a faculty in the department of Computer Science and Engineering at Thapar University, Patiala. He received his B.S., M.S. and Doctorate in 1991, 2001 and 2008, respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engg. College, Gorakhpur from 1991 to 1996. He joined Thapar University in 1996 and is presently associated with the same Institute. He has been a visiting faculty to many institutions. He has published over 100 papers in referred journals and conferences (India and Abroad). He has chaired various sessions in the International and National Conferences. He is active member of MIEEE, MACM, MISCI, LMCSI, MIETE, GMAIMA. He is a certified software quality auditor by MoCIT, Govt. of India. His research interests include wireless networks, routing algorithms and mobile clouds.

Gaurav Sharma received his PhD and M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. He had received M. Sc. as well as B. Sc. degree from CCS University, Meerut, India. He is an active member of IEEE and ACM. Presently he is working as an Asst. Professor at Amity University, India. His area of interests is routing and security in Ad hoc networks.

Murari Mandal was born in India, in 1990. He received the B.E. degree in Computer Science from BITS Pilani, India, in 2011 and M.E. degree in Software Engineering from Thapar University, India, in 2015. He has worked as Research Assistant in Computer Science department of BITS Pilani from 2015 to 2016. In 2016, he joined the Computer Engineering Department, MNIT Jaipur, as a Research Scholar. His current research interests include computer vision, image/video processing, machine learning, real-time systems, cryptography and sensor networks.