International Journal of Information & Network Security (IJINS)
Vol.1, No.3, August 2012, pp. 200~206
ISSN: 2089-3299

An Efficient ID-Based Proxy Signcryption Scheme

G. Swapna*, P.V.S.S.N. Gopal*, T. Gowri, P. Vasudeva Reddy***
* Department of Engineering Mathematics, Andhra University
** Department of Electronics and Communication Engineering, GITAM University

Article Info

Article history:

Received June 30th, 2012
Revised July 10th, 2012
Accepted July 22th, 2012

Keyword:

Identity-Based Cryptography
Proxy Signcryption
Public-Verifiability
Forward Security
Bilinear Pairings

ABSTRACT

Signcryption is a cryptographic primitive that performs encryption and signature in a single logical step, at lower computational cost and communication over heads than the signature-then-encryption. Proxy signcryption schemes are variations of ordinary signcryption schemes and have been useful in many applications where the delegation of rights is quite common. By combining the functionalities of proxy signature scheme and signcryption scheme, in this paper, we proposed a new ID-based proxy signcryption scheme which offers both public verifiability and forward security. The security requirements and performance of the proposed scheme are analyzed.

Corresponding Author:

P. Vasudeva Reddy,
Department of Engineering Mathematics, Andhra University, Visakhapatnam-530003,
Andhra Pradesh, INDIA.
Email: vasucrypto@yahoo.com

1. INTRODUCTION

The proxy signature is a cryptographic primitive and the first proxy signature is introduced by Mambo, Usuda and Okamoto [1]. The scheme allows an entity, called the original signer, to delegate another entity, called a proxy signer, to sign messages on its behalf. Proxy signature has found numerous practical applications, particularly in distributed computing where delegation of rights is quite common, such as e-cash systems, global distribution networks, grid computing, mobile agent applications, and mobile communications. A secure proxy signature scheme should satisfy the following five requirements: verifiability, strong Unforgeability, strong Identifiability, strong undeniability, prevention of misuse [1, 2].

In the areas of computer communications and electronic transactions, one of the important topics is how to send data in confidential and authenticated way. Usually, the confidentiality of delivered data is provided by encryption algorithm, and the authentication of messages is guaranteed by digital signatures. In 1997, Zhang [3] proposed a cryptographic primitive, called Signcryption, to achieve the combined functionalities of digital signatures and encryption in an efficient manner. Many researchers have been proposed variations of signcryption schemes [4]. One of these is a proxy signcryption scheme which is efficiently combines a proxy signature scheme with signcryption. Proxy signcryption scheme allows an entity to delegate its authority of signcryption to a trusted agent. The proxy signcryption scheme is useful for applications that are based on unreliable datagram style network communication model where messages are individually signed and not serially linked via a session key to provide authenticity and integrity. The first proxy signcryption scheme was proposed by Gamage et.al [5] in the traditional PKI based setting.

In 1984, Shamir [6] first proposed the idea of ID-based public key cryptography (ID-PKC) to simplify key management procedure of traditional certificate-based PKI. In ID-PKC, an entity's public key is directly derived from certain aspects of its identity, such as an IP address belonging to a network host or an e-mail address associated with a user. Private keys are generated for entities by a trusted third party called a private key generator (PKG). The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the problems associated with them. In 2001, due to the contribution of Boneh et al. [7], a rapid development of ID-PKC has taken place. Using bilinear pairings, many new ID-based signature schemes [8-11] and signcryption schemes [12-18] have been proposed. With these ID-based signature schemes and signcryption schemes a lot of new extensions such as proxy signcryption, blind signcryption, ring signcryption, multi signcryption etc, have been proposed in the literature [4].

The basic idea of ID-based proxy signcryption scheme is as follows. The original signcrypter sends a specific message with its signature to the proxy signcrypter, who then uses this information to construct a proxy private key. With the proxy private key, the proxy signcrypter can generate proxy signcryption by employing a specified standard ID-based signcryption scheme. When a proxy signcryption is given, a verifier checks its validity according to the corresponding standard ID-based signcryption verification procedure. Recently, in 2004, Li-Chen [19] proposed an ID-based proxy signcryption scheme. However, their scheme is based on the Libert and Quister signcryption scheme [13], which does not satisfy the security requirements at the same time.

In 2005, Wang and Cao [20] proposed an ID-based proxy signature and proxy signcryption scheme, which is based on the Chen-Lee signcryption scheme [15], and is efficient than Li-Chen scheme [19] in terms of computational point of view. In 2005, Wang and Cao [21] proposed another ID-based proxy signcryption scheme from bilinear pairings, which uses Zhang's proxy signature scheme [22] as the base scheme, and is more efficient than Li-Chen scheme[19] in computational overhead. In the same year 2005, Wang et al. [23] proposed an efficient ID-based proxy signcryption scheme with forward security and public verifiability.

In this paper we proposed an ID-based proxy signcryption (ID-PSC) scheme from bilinear pairings. This scheme is public-verifiable, forward secure and is much more efficient when compared with the above schemes in terms of computational overhead. The rest of this paper is organized as follows. In Section 2, we first review some basic concepts of bilinear pairings. Syntax and security requirements of our ID-PSC scheme are presented in Section 3. We proposed our ID-based proxy signcryption scheme in Section 4. Security and efficiency analysis of the ID-PSC scheme are presented in Section 5. Finally Section 6 concludes this paper.

2. PRELIMINARIES

In this section, we briefly review bilinear pairings and some computational problems.

2.1. Bilinear Pairings

Bilinear pairing is an important primitive and has been widely adapted in many positive applications in cryptography. Let G_1 be an additive cyclic group with a prime order q and G_2be a multiplicative cyclic group with the same order q. G_1 is a subgroup of the group of points on an elliptic curve and P is the generator of G_1. G_2 is a subgroup of the multiplicative group over a finite field. A bilinear pairing is a map $\hat{e}: G_1 \times G_1 \longrightarrow G_2$ which satisfies the following properties.

- **Bilinear:** $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$ for all $P \in G_1$ and $a, b \in Z_q^*$.
- **Non – degenerate**: There exists $P, Q \in G_1$, such that $\hat{e}(P, Q) \neq 1$.
- **Computability:** There exists an efficient algorithm to compute $\hat{e}(P, Q)$, for all $P, Q \in G_1$.

We call such a bilinear map $\hat{e}$ as an admissible bilinear pairing, and the Weil pairing in elliptic curve can give a good implementation of the admissible pairing [7].

2.2. Computational Problems

Now, we give some computational problems which will form the basis of security for our ID-PSC scheme.

- **Computational Diffie–Hellman Problem (CDHP):** The CDHP in G_1 is such that given (P, aP, bP) with uniformly random choices of $a, b \in Z_q^*$, to compute abP.
- **Computational Bilinear Diffie-Hellman Problem (CBDHP):** The CBDHP is such that given (P, aP, bP, cP) with uniformly random choices of $a, b, c \in Z_q^*$, to compute $\hat{e}(P, P)^{abc}$.
- **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.

3. SYNTAX AND SECURITY REQUIREMENTS OF THE PROPOSED ID-PSC SCHEME

In this section we present the syntax and security requirements of the proposed scheme.

3.1. Syntax of the ID-PSC Scheme

The ID-based proxy signcryption scheme (ID-PSC scheme) can be viewed as the combination of a general proxy signature and an Id-based signcryption scheme. Let A be the original signcrypter / sender with the identity ID_A and the private key S_{ID_A}. He delegate his signing rights to a proxy signcrypter /sender B with identity ID_B and the private key S_{ID_B}. A warrant m_ω is used to delegate signing rights. Now we give a formal model for our ID-based proxy signcryption scheme. Our scheme consists of the following algorithms:

- **Setup:** On input security parameter 1^k, PKG creates and publishes system parameters and keeps a master key as secret, which is known only by PKG.
- **Extract:** Given an identity ID of any entity, the PKG computes the public key and corresponding secret key and sends it to the corresponding entity through a secure channel.
- **Proxy delegation:** This is an interactive algorithm between D and P owned by the original signer and the proxy signer. The input of each algorithm includes the public key of the original signer ID_A. The algorithm D also takes the secret key S_{ID_A} as input. The algorithm P also takes as input the secret key S_{ID_B} of the proxy signer.

  As a result of the interaction, the proxy signer obtains a proxy signcryption key S_{Pro} that will use to signcrypt the messages on behalf of the original signcrypter.
- **Proxy signcryption:** The proxy signcryption algorithm, that takes as a proxy signcryption key S_{Pro}, the receiver identity ID_R, a message M, a warrant m_ω as input; and outputs a proxy signcryption text(ciphertext) σ.
- **Unsigncryption:** The Unsigncryption algorithm, which takes the identity of original sender ID_A, identity of the proxy sender ID_B, a message M, a warrant m_ω as input; output "accept" if the proxy signcryption is valid, or 'reject' otherwise.

3.2. Security Requirements of our ID-PSC Scheme

A secure ID-based proxy signcryption scheme should satisfy the following requirements.

1. **Verifiability:** From the proxy signcryption text, the recipient can be convinced of original sender's agreement on the signcrypted message.
2. **Strong Unforgeability:** The original sender and other third parties can't create a valid proxy signcryption text.
3. **Strong Identifiability:** Any one can determine the identity of the corresponding proxy sender from the proxy signcryption text.
4. **Prevention of Misuse:** The proxy sender can't use the proxy key for other purposes than generating a valid proxy signcryption text.
5. **Confidentiality:** Except the recipient, no one can't extract the plaintext from the proxy signcryption text.
6. **Non-repudiation:** The recipient can efficiently prove to any third party that the message is indeed originated from a specific sender on behalf of an original sender.
7. **Forward Security:** An attacker cannot reveal the messages signcrypted before even with the knowledge of the sender's private key.
8. **Public Verifiability:** The origin of the cipher text can be verified by any third party without knowing the recipient's private key.

4. PROPOSED ID-PSC SCHEME

In this section we propose an ID- based proxy signcryption (ID-PSC) scheme which uses bilinear pairings over elliptic curves. This scheme allows the original sender A to delegate the signcryption capability to the proxy signcrypter B. The proxy signcrypter B signcrypt the messages on the behalf of the original sender A. After receiving the proxy signcryption text, anyone can verify the validity of the proxy signcryption.

4.1. Setup

Given a security parameter k, n, the PKG chooses two cyclic groups G_1 and G_2 of prime order q, a generator P of G_1 , a bilinear map $\hat{e}: G_1 \times G_1 \longrightarrow G_2$ and a hash functions $H_1: \{0,1\}^* \longrightarrow G_1$, $H_2: \{0,1\}^* \longrightarrow z_q^*$, $H_3: \{0,1\}^* \times G_1^3 \longrightarrow z_q^*$. PKG chooses a master key $s \in Z_q^*$ and computes $P_{Pub} = sP \in G_1$ as a PKG's public key. It also chooses a secure symmetric key pair (E, D). The PKG publishes the system parameters as $Params: \{k, n, G_1, G_2, P, P_{Pub}, \hat{e}, H_1, H_2, H_3, E, D\}$.

4.2. Key Extract

Given an identity ID_i, PKG computes $Q_{ID_i} = H_1(ID_i) \in G_1$ and the corresponding private key $S_{ID_i} = sQ_{ID_i} \in G_1$. Let (Q_{ID_A}, S_{ID_A}) be the original sender's key pair, (Q_{ID_B}, S_{ID_B}) be the proxy sender's key pair, and (Q_{ID_R}, S_{ID_R}) be the receiver's key pair.

4.3. Proxy Delegation

To delegate the signcrypting capacity to a proxy signcrypter, original signcrypter makes a signed warrant m_ω, there is an explicit description of the delegation rights and information of the original signcrypter and proxy signcrypter in the warrant m_ω such that a verifier can use it as a part of verification information, and sends it to the proxy signcrypter.

The original sender chooses $r_\omega \in Z_q^*$ and sets $U_\omega = r_\omega P \in G_1$ and $H_\omega = H_2(Q_{ID_A}||m_\omega||U_\omega)$ and then computes $V_\omega = S_{ID_A} + r_\omega H_\omega P_{Pub} \in G_1$. Then he sends $(m_\omega, U_\omega, V_\omega)$ to the proxy sender via a secure channel.

4.4. Proxy Key Generation

After receiving the proxy certificate $(m_\omega, U_\omega, V_\omega)$, the proxy sender B verifies the validity of the signature on m_ω as follows.

1. He computes $H_\omega = H_2\left(Q_{ID_A} \| m_\omega \| U_\omega\right)$.
2. Accept the signature iff $\hat{e}(P, V_\omega) = \hat{e}(P_{pub}, Q_{ID_A} + H_\omega U_\omega)$.
   Proof of correctness: $\hat{e}(P, V_\omega) = \hat{e}\left(P, sQ_{ID_A} + H_\omega r_\omega sP\right)$
   $= \hat{e}(P_{pub}, Q_{ID_A} + H_\omega r_\omega P)$
   $= \hat{e}(P_{pub}, Q_{ID_A} + H_\omega U_\omega)$.
3. For a valid delegation, the proxy sender computes a proxy private key as $S_{Pro} = H_2\left(Q_{ID_A} \| m_\omega \| U_\omega\right) S_{ID_B}$.

4.5. Proxy Signcryption

To signcrypt a plaintext $M \in \{0,1\}^n$ to a receiver, on behalf of the original signcrypter A, the proxy signcrypter B does the following.

1. Pick $r \in Z_q^*$ and compute $U = rP \in G_1$.
2. Compute $\hat{\alpha} = \hat{e}(P_{pub}, Q_{ID_R})^r \in G_2$.
3. Compute $\alpha_{2=} H_2(\hat{\alpha})$.
4. Compute C = $E_{\alpha_2}(M)$.
5. Compute $h = H_3\left(C, U, Q_{ID_B}, Q_{ID_R}\right)$.
6. Compute $V = S_{Pro} + rhP_{pub} \in G_1$.
7. Send the resultant signcryption text (ciphertext) on message M as $\sigma = (m_\omega, U_\omega, U, V, C)$ to the receiver.

4.6. Unsigncryption

Upon receiving the signcryption text σ from the proxy signcrypter B, the receiver R, does the following.

1. Compute $\hat{\alpha}' = \hat{e}\left(U, S_{ID_R}\right)$.
2. Compute $\alpha_2' = H_2(\hat{\alpha}')$.
3. Compute $M = D_{\alpha_2'}(C)$.
4. Compute $h = H_3(C, U, Q_{ID_B}, Q_{ID_R})$.
5. Accept the signcryption iff $\hat{e}(P, V) = \hat{e}\left(P_{Pub}, hU + H_2\left(Q_{ID_A} \| m_\omega \| U_\omega\right) Q_{ID_B}\right)$.

5. ANALYSIS OF THE PROPOSED SCHEME

In this section first we present the proof of correctness and then we discuss the security and efficiency analysis of the proposed ID-PSC scheme.

5.1. Proof of Correctness

The following equations gives the correctness of the proposed scheme.

$$\hat{e}(P, V) = \hat{e}\left(P, S_{Pro} + rhP_{pub}\right)$$
$$= \hat{e}\left(P, H_2\left(Q_{ID_A} \| m_\omega \| U_\omega\right) S_{ID_B} + rhP_{pub}\right)$$
$$= \hat{e}\left(P_{Pub}, hU + H_2\left(Q_{ID_A} \| m_\omega \| U_\omega\right) Q_{ID_B}\right).$$

5.2. Security Analysis

In the following we discuss the security requirements, as discussed in Section 3.2, of the proposed ID-PSC scheme.

1. **Verifiability:** From the proxy unsigncrypting phase, the receiver can be convinced that the proxy sender has the original sender's signature on the warrant ω. The warrant ω also contains the identity information of the original sender, proxy sender and the limit of delegated signcrypting capacity etc. So

the receiver can be convinced of the original sender's agreement on the signcrypted message. Thus the scheme satisfies the security requirement 1

2. **Strong Unforgeability:** Because the proxy sender uses his private key to generate the proxy signcryption key $S_{Pro} = H_2(Q_{ID_A} \| m_\omega \| U_\omega) S_{ID_B}$, so that no one can get the proxy signcryption key S_{Pro} except the proxy sender himself. To create a valid proxy signcryption, one needs to compute the value of r and S_{Pro}. But due to intractability of DLP, it is difficult to compute r and S_{ID_B}. Thus except the proxy signcrypter, no one can create a valid proxy signcryption text. Thus our scheme is unforgeable.
3. **Strong Identifiability:** It contains the warrant ω in a valid proxy signcryption text and any one can determine the identity of the corresponding proxy sender from the warrant ω. So the scheme satisfies the security requirements 3.
4. **Prevention of Misuse:** In our proxy signcryption scheme, using the warrant ω, we have determined the limit of the delegated signcrypting capacity in the warrant and then the proxy sender can't signcrypt the messages that have not been authorized by the original sender. So the scheme satisfies the requirement 4.
5. **Confidentiality:** Except the receiver, anyone else can't extract the plaintext M from the proxy signcryption text $(m_\omega, U_\omega, U, V, C)$. For getting the message M, the attacker has to decrypt the ciphertext C directly. To do so, the attacker has to obtain the key α_2, since $(E_{\alpha_2}(.), D_{\alpha_2'}(.))$ is assumed to be an ideal symmetric key encryption/decryption algorithm pair. $\hat{\alpha} = \hat{e}(P_{pub}, Q_{ID_R})^r = \hat{e}(U, S_{ID_R})$, however, the attacker can't get the value of $\hat{e}(U, S_{ID_R})$ from the known values. This is the BDH problem which is intractable in security community [7]. Therefore, we conclude that our scheme meets the security requirement 5.
6. **Non-Repudiation:** A third party can settle repudiation disputes in a similar manner to the public proxy verification algorithm. So the scheme satisfies the security requirement 6.
7. **Forward Security:** Unsigncryption requires the knowledge of r. But, due to intractability of the DLP, it is difficult to compute r from V even with the knowledge of h and S_{ID_B}. Thus the proposed scheme is forward secure.
8. **Public Verifiability:** Since the knowledge of the plaintext M is not required for the public verification of message's origin, any third party can be convinced of the message's origin by verifying the equality $\hat{e}(P, V) = \hat{e}(P_{Pub}, hU + H_2(Q_{ID_A} \| m_\omega \| U_\omega) Q_{ID_B})$ holds. Thus the origin of the ciphertext can be verified without the help of recipient in our scheme. Hence the proposed scheme is public verifiable and meets the security requirement 8.

5.3. Efficiency Analysis

In this section, we compare the efficiency of our ID-PSC scheme with the related schemes such as Wang-Li [23] and Wang-Cao [21] schemes from computation overhead.

Here we denote A by a point addition in G_1, E by an exponentiation in G_2, and P by a computation of pairing.

In the table 1 below we enumerate the various operations necessary for each.

Table1. Comparisons of our scheme with Wang-Li and Wang-Cao schemes

Algorithm	Our ID-PSC Scheme	Wang-Li Scheme[23]	Wang-Cao scheme[21]
Proxy Key Generation	2A+4M+2P	1A+3M+1E+3P	2A+3M+2E+3P
Proxy Signcryption	1A+2M+1E+1P	2A+1M+2E+2P	1A+2M+2E+2P
Proxy Unsigncryption	1A+2M+3P	4E+8P	1A+3E+3P

In our scheme, the three algorithms Proxy Generation, Proxy Signcryption, and Proxy Unsigncryption totally requires 4A+8M+1E+6P, while Wang-Li scheme totally requires 3A+4M+7E+13P and Wang-Cao scheme totally requires 4A+5M+7E+8P. We note that the computation of the pairing is most time consuming. Although there has many papers discussing the complexity of the pairing [24] and how to speed up the pairing computation, the computation of the pairing still remains time-consuming. Thus our scheme only needs 6 pairing computations, while Wang-Li scheme needs 13 pairing computations and Wang-Cao scheme needs 8 pairing computations. So, our scheme is much more efficient than Wang-Li and Wang-Cao scheme.

6. CONCLUSION

In this paper, we proposed a public verifiable and forward secure ID- based proxy signcryption (ID-PSC) scheme. This scheme allows the original signcrypter to delegate the signcryption capability to the proxy signcrypter. The proxy signcrypter signcrypt messages on the behalf of the original signcrypter. After receiving the proxy signcryption text, anyone can verify the validity of the proxy signcryption. The proposed scheme is very useful in some practical applications where the delegation of signcryption rights is quite common. We have discussed the security requirements of the scheme with the assumptions that the BDH and DL problems are intractable. In terms of computational point of view, our scheme only needs 6 pairing computations, while Wang-Li scheme needs 13 pairing computations and Wang-Cao scheme needs 8 pairing computations. So, the proposed ID-PSC scheme is much more efficient than Wang-Li and Wang-Cao schemes.

REFERENCES

[1] M. Mambo, K. Usuda, E. Okamoto, "Proxy Signatures: Delegation of the Power to Sign Messages," *IEICE Trans. on Fundamentals*, E79-A (9), pp.1338–1354, 1996.

[2] B. Lee, H. Kim, K. Kim, "Strong Proxy Signature and its Applications," In *Proc. of the 2001 Symposium on Cryptography and Information Security (SCIS)*, Vol. 2(2), pp.603-608, 2001.

[3] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption)," *Advances in Cryptology*, LNCS, Vol. 1294. Springer-Verlag, pp.165–179, 1997.

[4] Fagen Li, M.K. Khan, "A Survey of Identity-Based Signcryption," *IETE Technical Review*, Vol. 28, No. 3, pp. 265-272, 2011.

[5] C. Gamage, J. Leiwo, Y. Zheng, "An Efficient Scheme for Secure Message Transmission Using Proxy-Signcryption," *22nd Australasian Computer Science Conference*, Springer- Verlag, pp. 420–431, 1999.

[6] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology-Crypto*, LNCS, Vol. 196. Springer-Verlag, pp. 47-53, 1984.

[7] D. Boneh, M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Advances in Cryptology-Crypto*, LNCS, Vol. 2139, Springer-Verlag, pp. 213-229, 2001.

[8] J. Beak, J. Newmarch, R. Safavi-Naini, W. Susilo, "A Survey of Identity-Based Cryptography," In *Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG 2004)*, pp. 95-102 (2004).

[9] M.C. Gorantla, R. Gangi Setti, A. Saxenal, "A Survey on ID- based Cryptographic Primitives," *IACR, Cryptology e-print Archive*, Report 2005 / 094, 2005. http:/eprint.iacr.org.

[10] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *Selected Areas in Cryptography: 9th Annual International Workshop*, LNCS, Vol. 2595. Springer-Verlag, pp.310–324, 2003.

[11] J.C. Cha, J.H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," In *Proc. of Public Key Cryptography*, LNCS, Vol. 2567. Springer-Verlag, pp.18–30, 2003.

[12] J. Malone Lee, "Identity based signcryption," In *Cryptology ePrint Archive*, Report 2002/098, 2002.

[13] B. Libert, J. Quisquater, "A New Identity Based Signcryption Scheme from Pairings," In *IEEE Information Theory Workshop*, pp.155-158, 2003.

[14] S.S.M. Chow, S.M. Yiu, L.C.K. Hui, K.P. Chow, "Efficient forward and provably secure id-based signcryption scheme with public verifiability and public cipher text authenticity," In *ICISC 2003*, LNCS, Vol. 2971, Springer-\ Verlag, pp. 352– 369, 2004.

[15] L. Chen, J.M. Lee, "Improved Identity-Based Signcryption," In *Proc. Of Public Key Cryptography*, LNCS, Vol. 3386, Springer- Verlag, pp. 362–379, 2005.

[16] P.S.L.M. Barreto, B. Libert, N. McCullagh, J.J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," In *Advances in Cryptology-ASIACRYPT 2005*, LNCS 3788, pp. 515–532, Springer-Verlag, 2005.

[17] S. S. D. Selvi, S. S. Vivek, C. P. Rangan, "Identity based public verifiable signcryption scheme," *Proc. ProvSec 2010*, LNCS, Vol 6402, Springer-Verlag, pp. 244-260, 2010.

[18] Prashant Kushwah, Sunderlal, "Efficient identity based public verifiable signcryption scheme," *IJCST*, Vol. 2, Issue3, pp. 513-518, 2011.

[19] X. Li, K. Chen, "Identity Based Proxy-Signcryption Scheme from Pairings," In *Proc. of the 2004 IEEE International Conference on Services Computing*, IEEE Computer Society, pp. 494-497, 2004.

[20] Qin Wang, Zhenfu Cao., "Efficient Id Based Proxy Signature and Proxy Signcryption from Bilinear Pairings," *CIS 2005*, Part II, LNAI 3802, Springer-Verlag, pp.167-172, 2005.

[21] Qin Wang, Zhenfu Cao.,"Two Proxy Signcryption Schemes from Bilinear Pairings," *CANS 2005*, LNCS 3810, Springer-Verlag, pp. 161–171, 2005.

[22] F. Zhang, K. Kim, "Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings," *Australasian Conference on Information Security and Privacy*, LNCS, Vol. 2727, Springer-Verlag, pp. 312–323, 2003.

[23] Meng Wang, Hui Li, Zhijing Liu, "Efficient Identity Based Proxy-Signcryption Schemes with Forward Security and Public Verifiability," *ICCNMC 2005*, LNCS 3619, Springer-Verlag, pp. 982 – 991, 2005.

[24] P.L.S.M. Baretto, H.Y. Kim, B. Lynn, M. Scott, "Efficient Algorithms for Pairing Based Cryptosystems," *Advances in Cryptology-Crypto 2002*, LNCS 2442, Springer-Verlag, pp. 354-368,2002.

BIOGRAPHY OF AUTHORS

Swapna received M.Sc (Mathematics) and M.Phil (Cryptography) from Andhra University, Visakhapatnam, Andhra Pradesh, India in 2005 & 2009 respectively. Presently she is working in the area of ID-Based cryptography for her Ph.D degree in Andhra University, Visakhapatnam, India.

P.V.S.S.N. Gopal received the M.Sc degree in Applied Mathematics and M.Phil in (Commutative Algebra) Mathematics from Pondicherry University, Pondicherry, India in 2001 and 2008 respectively. He is presently pursuing Ph.D in Andhra University, Visakhapatnam, India. His area of interests includes Elliptic Curve Cryptography.

T. Gowri received B.Tech from Nagarjuna University, and M. Tech from Jawaharlal Nehru Technological University. She is currently working as an Associate professor in the department of Electronics and Communication Engineering, GIET, GITAM University, Visakhapatnam, A.P, India. Her research interests include Digital Information Systems and Computer Electronics, Digital Image Processing and Information Security.

P. Vasudeva Reddy received M.Sc (Mathematics), Ph.D (Cryptography) from S.V. University, Tirupati, M. Tech (CST-Networks) from Andhra University, India. He is currently working as an Associate professor in the department of Engg. Mathematics, College of Engineering, Andhra University, Visakhapatnam, India. His field of interest includes Algebra & Number theory Applications, secret sharing, and Cryptography. He has several publications in national and international reputed journals. He is a life member of Cryptology Research Society of India (CRSI).