An Efficient ID-Based Proxy Signcryption Scheme without Bilinear Pairings

Hassan M. Elkamchouchi
Elec. Eng. Dept, Fac. of Eng ,
Alexandria
Alexandria
Egypt

Yasmine Abouelseoud
Eng. Math. Dept, Fac. of Eng ,
Alexandria
Alexandria
Egypt

Eman F. Abu Elkhair
Elec. Eng. Dept, Fac. of Eng ,
Kafr Elsheikh
Kafr Elsheikh
Egypt

ABSTRACT

Signcryption is a cryptographic primitive which simultaneously provides both confidentiality and authenticity in a single logical step. Signcryption based on elliptic curves provides the same level of security using smaller keys compared to schemes based on the discrete logarithm problem over finite fields. Identity-based cryptography serves as an efficient alternative to the traditional certificate-based cryptosystems. The idea of identity-based cryptography is to enable a user to use any arbitrary string that uniquely identifies him as his public key. In a proxy signcryption scheme, an original signer delegates his signing power to a proxy agent, who signcrypts a message on behalf of him. This paper introduces a new identity based proxy signcryption scheme without bilinear pairings. Its security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) with a reduced computational complexity compared to other schemes in literature. In this proposed scheme, the receiver is the only one who can verify the origin of the ciphertext. Moreover, in this scheme, an authorized proxy signcrypter can create valid proxy signatures after verifying the identity of the original signcrypter. The proposed scheme achieves the various desirable security requirements.

General Terms

Cryptography, Security.

Keywords

Identity-Based Cryptography, Proxy Signcryption, Elliptic Curve Discrete Logarithm Problem

1. INTRODUCTION

Confidentiality, integrity, authentication, and non-repudiation are the most important security requirements for many applications. Confidentiality is keeping information secret from all other than those who are authorized to see it. Integrity is ensuring that the information has not been altered by unauthorized entities. Authentication is the assurance that the communicating party is the one that it claims to be. Non-repudiation is preventing the denial of previous commitments or actions. Encryption can achieve confidentiality and digital signature can achieve the integrity, authentication, and non-repudiation. If we need to achieve simultaneously all theses goals, the traditional approach is first to sign a message and then to encrypt it, which is called the sign-then-encrypt or signature-then-encryption approach. In 1997, Zheng [1] proposed a new cryptographic primitive called signcryption that fulfills both the functions of a digital signature and public key encryption simultaneously, at a cost significantly lower than that required by the traditional signature-then-encryption approach. Several efficient signcryption schemes [2, 3, 4] have been proposed since 1997. Signcryption has found many applications, such as secure electronic transaction protocols, mobile agent protocols, key management, and routing protocols. The original scheme in [1] is based on the discrete logarithm problem but no security proof was given. Zheng's original scheme was only proven secure by Baek et al. [5], who also described a formal security model in a multi-user setting.

In the traditional signcryption schemes, the public key of a user is essentially a random bit string picked from a given set. So, the signcryption does not provide the authorization of the user by itself. This problem can be solved via a certificate, which provides an unforgeable and trusted link between the public key and the identity of the user by means of the signature of a certificate authority (CA). There is a hierarchical framework that is called public key infrastructure (PKI) which issues and manages certificates. However, the certificates management, including revocation, storage, distribution, and the computational cost of certificates verification are the main difficulties against traditional PKI.

To simplify the key management procedures, Shamir [6] proposed the concept of identity-based cryptography (IBC) in 1984. The idea of IBC is to get rid of certificates by allowing a user's public key to be any binary string that uniquely identifies the user. Examples of such strings include email addresses and IP addresses. Malone-Lee extended the signcryption idea to identity-based cryptography and presented an identity-based signcryption scheme [7]. Several practical identity-based schemes [8, 9, 10, 11] have been devised since 1984. To date, several identity-based signcryption schemes have been developed in literature [12, 13, 14, 15, 16, 17, 18].

The main practical benefit of IBC is in greatly reducing the need for public key certificates. IBC uses a trusted third party called private key generator (PKG). The PKG generates the private keys of all of its users, so a user can decrypt/sign only if the PKG has given a secret key to it. Thus, certification is implicit, and hence this reduces the amount of storage and computation [19].

Many researchers have proposed a variety of identity-based signcryption schemes [20]. One of these variants is an identity- based proxy signcryption scheme which combines a proxy signature scheme with an encryption mechanism [21]. A proxy signcryption scheme allows an entity to delegate its authority of signcryption to a trusted agent. Proxy signcryption scheme is useful for applications that are based on unreliable datagram style network communication model, where the 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 [22] in the traditional PKI based setting.

This paper proposes a new identity based proxy signcryption scheme in which the sender delegates his signing rights to a trusted proxy. The scheme has a low computational cost and is less time consuming when compared with the scheme in [21].

The paper is organized as follow. In the next section, the hard computational problems are discussed. Section 3 introduces the syntax of a generic identity-based proxy signcryption scheme (ID-PSC). Section 4 introduces the security requirements of any identity-based proxy signcryption scheme. In Section 5, the proposed identity-based proxy signcryption scheme is discussed. Section 6 introduces the performance analysis of the proposed scheme. Section 7 shows the comparison between the proposed scheme and the scheme in [21]. Section 8 concludes the paper and finally Section 9 is the list of references used.

2. COMPUTATIONALLY HARD PROBLEMS

Here, the hard computational problems, upon which the security of the proposed scheme relies, will be discussed [23,24]:

2.1 The Discrete Logarithm Problem (DLP)

Let p and q be two large primes satisfying $q \mid p-1$, and g a generator of order q over $GF(p)$. The discrete logarithm problem is, given an instance (y, p, q, g) where $y = g^x \bmod p$ for some $x \in Z_q$, to derive x.

2.2 Discrete Logarithm (DL) Assumption

A probabilistic polynomial-time algorithm (PPT) B is said to (t, ε) break the DLP if given a DLP instance (y, p, q, g) where $y = g^x \bmod p$ for some $x \in Z_q$, B can derive x with probability ε after running at most t steps. The probability is taken over the uniformly and independently chosen instance and over the random bits consumed by B.

Definition 1 The (t, ε) DL assumption holds if there is no probabilistic polynomial-time adversary that can (t, ε) break the DLP.

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

An elliptic curve group is described using additive notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group G of points on the elliptic curve over Z_p, find a number k such that $kP = Q; k$ is called the discrete logarithm of Q to the base P .

3. SYNTAX OF THE ID-PSC SCHEME

A generic identity-based proxy signcryption (ID-PSC) scheme consists of the following algorithms[21]:

3.1 Setup

This is a probabilistic polynomial-time (PPT) algorithm run by a PKG that takes as input 1^k and outputs system parameters, including a master public key pk and a master private key sk. Here, k is a security parameter.

3.2 Extract

This is a key generation algorithm run by the PKG that takes as input the master private key sk and an identity $ID_u \epsilon \{0,1\}^*$, and outputs the corresponding private key S_u.

3.3 Proxy Delegation

This is an interactive algorithm between the original signer and the proxy signer. The input to the algorithm includes the public key of the original signer ID_S . This algorithm also takes the secret key of original signcrypter and the secret key of the proxy signcrypter as input. As a result of the interaction, the proxy signer obtains a secret proxy signcryption key S_p that will be used to signcrypt the messages on behalf of the original signcrypter together with a warrant indicating his signing rights.

3.4 Proxy Signcrypt

This is a PPT algorithm that takes as input a plaintext message m, a receiver's identity ID_r, the warrant m_w where m_w is a warrant consisting of the identifiers of the original and the proxy agents, the delegation duration and so on , and a proxy private key S_p, and outputs a ciphertext

$$\sigma = \text{Signcrypt}(m, m_w, S_p, ID_r).$$

3.5 Proxy Unsigncrypt

This is a deterministic algorithm that takes as input a ciphertext σ, the receiver's private key S_r, the warrant m_w, the sender's identity ID_s, and the proxy identity ID_p and outputs the original message m or the rejection symbol $\perp$ if σ is an invalid ciphertext: $m = \text{Unsigncrypt}(\sigma, m_w, S_r, ID_s, ID_p)$.

4. SECURITY REQUIREMENTS OF A ID-PSC SCHEME

A secure ID-based proxy signcryption scheme should satisfy the following requirements [23].

4.1 Verifiability

From the proxy signcryption text, the recipient can be convinced of original sender's agreement on the signcrypted message.

4.2 Unforgeability

The original sender and other third parties cannot create a valid proxy signcryption text.

4.3 Identifiability

Anyone can determine the identity of the corresponding proxy sender from the proxy signcryption text.

4.4 Prevention of Misuse

The proxy sender cannot use the proxy key for other purposes than generating a valid proxy signcryption text.

4.5 Confidentiality

Except the recipient, no one can extract the plaintext from the proxy signcryption text.

4.6 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.

4.7 Forward Security

An attacker cannot learn messages signcrypted before even with the knowledge of the sender's private key.

4.8 Public Verifiability

The origin of the ciphertext can be verified by any third party without knowing the recipient's private key.

5. THE PROPOSED IDENTITY-BASED PROXY SIGNCRYPTION SCHEME

5.1 Setup

Given the security parameter k, the key generation center (KGC) chooses a group G of a prime order q, q a large prime number, where $q > 2^k$, (a, b) two integer elements which are smaller than q and satisfy $(4a^3 + 27b^2) \bmod q \neq 0$. E is the selected elliptic curve over finite field $F_p : y^2 = (x^3 + ax + b) \bmod p$, where p is a large prime number. P is the base point of order q of the group G. Also, O is the point at infinity. The KGC selects two cryptographic one way hash functions $H : \{0,1\}^* \to Z_q$ and $h : \{0,1\}^k \times Z_q \to Z_q$.

5.2 Key Generation

The KGC selects a random number s as the master secret key and computes the master public key $R = s.P$. The KGC keeps s secret and publishes the system parameters params: $\{k, G, P, R, H, h\}$. The KGC generates the secret and public keys of the sender, proxy and receiver then sends the secret keys through a secure channel and publishes the public keys and the identities. The KGC calculates the secret keys for the sender, the proxy and the receiver respectively as follows: $x_S = (H(ID_S).s) \bmod q$, $x_p = (H(ID_p).s) \bmod q$ and $x_r = (H(ID_r).s) \bmod q$. The KGC calculates the public keys as follows; $Q_s = x_s.R$; the sender's public key, $Q_p = x_p.R$; the proxy's public key and $Q_r = x_r.R$; the receiver's public key.

The proposed ID-based proxy signcryption scheme is shown in Figure 1.

5.3 Proxy-Credential-Generation (PCG)

The original signer chooses a random number $d \in [1, q-1]$ and computes:

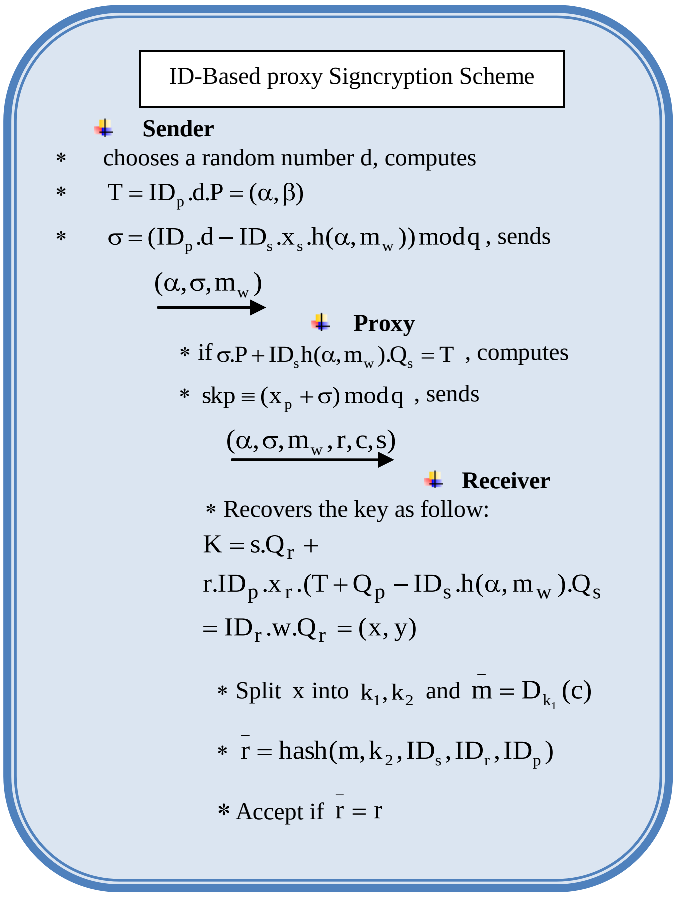
- $T = ID_p.d.P = (\alpha, \beta)$
- $\sigma = (ID_p.d - ID_s.x_s.h(\alpha, m_w)) \bmod q$

The original signer sends (α, σ, m_w) to the proxy. The proxy checks the validity of the signature as follows: If $\sigma.P + ID_s h(\alpha, m_w).Q_s = T$, then the proxy computes the secret proxy key. Otherwise, the proxy requests a new (α, σ, m_W)-tuple.

The correctness of the verification of equation is demonstrated below:

$$RHS = \sigma.P + ID_s.h(\alpha, m_w).Q_s$$
$$= (ID_p.d - ID_s.x_s.h(\alpha, m_w)).P + ID_s.h(\alpha, m_w).Q_s$$
$$= ID_p.d.P - ID_s.x_s.h(\alpha, m_w).P + ID_s.x_s.h(\alpha, m_w).P$$
$$= ID_p.d.P = T = LHS$$

After the proxy authenticates the original signer, the proxy computes the secret proxy key as: $skp \equiv (x_p + \sigma) \bmod q$



ID-Based proxy Signcryption Scheme

Sender

* chooses a random number d, computes

* $T = ID_p.d.P = (\alpha, \beta)$

* $\sigma = (ID_p.d - ID_s.x_s.h(\alpha, m_w)) \bmod q$, sends

$\xrightarrow{(\alpha, \sigma, m_w)}$

Proxy

* if $\sigma.P + ID_s h(\alpha, m_w).Q_s = T$, computes

* $skp \equiv (x_p + \sigma) \bmod q$, sends

$\xrightarrow{(\alpha, \sigma, m_w, r, c, s)}$

Receiver

* Recovers the key as follow:

$K = s.Q_r +$
$r.ID_p.x_r.(T + Q_p - ID_s.h(\alpha, m_w).Q_s$
$= ID_r.w.Q_r = (x, y)$

* Split x into k_1, k_2 and $\bar{m} = D_{k_1}(c)$

* $\bar{r} = hash(m, k_2, ID_s, ID_r, ID_p)$

* Accept if $\bar{r} = r$

Fig 1: ID-Based proxy Signcryption Scheme

5.4 Proxy Signcryption

The sender chooses a random number w and computes:

– $K = ID_r.w.Q_r = (x, y)$

– Split x into k_1, k_2

– $c = E_{k_1}(m)$

– $r = hash(m, k_2, ID_s, ID_r, ID_p)$

– $s = (ID_r.w - ID_p.r.skp) \bmod q$

– The sender sends $(\alpha, \sigma, m_w, r, c, s)$ to the receiver

5.5 Unsigncryption Phase

The receiver recovers the key K as follows:

$$K = s.Q_r + r.ID_p.x_r.(T + Q_p - ID_s.h(\alpha, m_w).Q_s$$
$$= ID_r.w.Q_r = (x, y)$$

– Split x into k_1, k_2

– $\bar{m} = D_{k_1}(c)$

– $\bar{r} = hash(m, k_2, ID_s, ID_r, ID_p)$

– If $\bar{r} = r$ the receiver accept the signature.

6. PERFORMANCE ANALYSIS

6.1 Correctness

The correctness of the key recovery equation is demonstrated below:

$$K = s.Q_r + ID_p.r.x_r.(T + Q_p - ID_s.h(\alpha, m_w)Q_s)$$
$$= (ID_r.w - ID_p.r.skp).Q_r + ID_p.r.x_r.T + ID_p.r.x_r.Q_p$$
$$- ID_p.r.x_r.ID_s.h(\alpha, m_w)Q_s$$

$$= ID_r.w.Q_r - ID_p.r.(x_p + \sigma).Q_r + ID_p.r.x_r.T + ID_p.r.x_r.Q_p -$$
$$ID_p.r.x_r.ID_s.h(\alpha, m_w)Q_s$$
$$= ID_r.w.Q_r - ID_p.r.(x_p + ID_p.d - ID_s.x_s.h(\alpha, m_w)).Q_r +$$
$$ID_p.r.x_r.T + ID_p.r.x_r.Q_p - ID_p.r.x_r.ID_s.h(\alpha, m_w)Q_s$$
$$= ID_r.w.Q_r - ID_p.r.x_p.Q_r - ID_p.r.ID_p.d.Q_r +$$
$$ID_p.r.ID_s.x_s.h(\alpha, m_w).Q_r + ID_p.r.x_r.T + ID_p.r.x_r.Q_p -$$
$$ID_p.r.x_r.ID_s.h(\alpha, m_w)Q_s$$
$$= ID_r.w.Q_r - ID_p.r.x_p.x_r.P - ID_p.r.ID_p.d.x_r.P +$$
$$ID_p.r.ID_s.x_s.h(\alpha, m_w).x_r.P + ID_p.r.x_r.ID_p.d.P$$
$$+ ID_p.r.x_r.x_p.P - ID_p.r.x_r.ID_s.h(\alpha, m_w)x_s.P) = ID_r.w.Q_r$$
$$= (x, y)$$

6.2 Security Analysis

In what follows, the security properties of the proposed scheme are investigated.

6.2.1 Verifiability

According to the proxy unsigncryption phase, the receiver can be convinced that the proxy sender has the original sender's signature on the warrant. The warrant also contains the identity information of the original sender, the proxy sender and the limit of the delegated signcrypting capacity etc. Therefore, the receiver can be convinced of the original sender's agreement on the signcrypted message. Thus, the scheme satisfies the verifiability requirement.

6.2.2 Unforgeability

Because the proxy sender uses his private key x_p to generate the proxy signcryption key $skp \equiv (x_p + \sigma) \bmod q$, no one can get the proxy signcryption key skp except the proxy sender himself. To create a valid proxy signcryption $s = (ID_r.w - ID_p.r.skp) \bmod q$, one needs to compute the value of w and skp. But due to the intractability of the ECDLP, it is difficult to compute w and skp. Thus, except the proxy signcrypter, no one can create a valid proxy signcryption text. Thus, the proposed scheme supports unforgeability.

6.2.3 Identifiability

The proxy signcrypted text $\delta = (\sigma, m_w, \alpha, r, s, c)$ contains the warrant m_w. Moreover, the verification equation

$$K = s.Q_r + ID_p.r.x_r.(T + Q_p - ID_s.h(\alpha, m_w)Q_s)$$

includes the original signcrypter public key Q_s and the proxy signcrypter public key Q_p. Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signature. So, the scheme satisfies the identifiability requirement.

6.2.4 Prevention of Misuse

In the proposed proxy signcryption scheme, using the warrant m_w, the limit of the delegated signcrypting capacity is clearly specified in the warrant and then the proxy sender cannot signcrypt the messages that have not been authorized by the original sender.

6.2.5 Confidentiality

The message is encrypted so that it can only be decrypted by the intended recipient in possession of the secret session key. Only the receiver can recover the key by which the encryption process is constructed because the receiver uses his secret key to recover the encryption /decryption key as follows:

$$K = s.Q_r + ID_p.r.x_r.(T + Q_p - ID_s.h(\alpha, m_w)Q_s)$$

Therefore, we conclude that the proposed scheme meets this security requirement.

6.2.6 Non-Repudiation

In this scheme, the original signer does not know the proxy signer's secret key x_p and the proxy signer does not know original signer's secret key x_s. Thus, neither the original signer nor the proxy signer can sign in place of the other party. Thus, the scheme provides non-repudiation.

6.2.7 Public Verifiability

After the receiver recovers the session key: $K = s.Q_r + ID_p.r.x_r.(T + Q_p - ID_s.h(\alpha, m_w)Q_s)$, he/she publishes the key to any third party who can verify the origin of the ciphertext.

7. COMPARATIVE STUDY

The performance of the proposed identity based proxy signcryption scheme based on the ECDLP is analyzed and compared to the scheme in [21]. It is found that the proposed scheme involves fewer computations than the scheme in [21]; that is, the proposed scheme is computationally more efficient than the other scheme in [21]. Moreover, the proposed scheme meets various security requirements. Table 1 defines the notation that will be used in the comparison. Table 2 shows the comparison between the proposed signcryption scheme and the scheme in [21].

8. CONCLUSION

This paper introduces an efficient identity based proxy signcryption scheme based on elliptic curve cryptography. This scheme has many applications such as in e-cash systems. Identity-based schemes resolve the problem of managing certificates in the traditional PKI cryptosystems.

The security properties of the proposed scheme are investigated revealing that it meets various security requirements. The use of a warrant facilitates identifying both the original as well as proxy agents. Additionally, warrants are used to specify the signing capacity of the proxy agent to prevent misuse of the delegation capability. Moreover, the proposed scheme is compared with the scheme in [21] and it is found that the proposed scheme reduces the computational burden so that it is more efficient.

Table.1. Time Abbreviations

Symbol	**Operation**
$T_{EC\text{-}mult}$	time required for executing multiplication operation on elliptic curve *E*
$T_{EC\text{-}add}$	time required for executing addition operation on elliptic curve *E*
T_{mult}	time required for executing modulus multiplication in a finite field
T_h	time required for executing one way dispersed row function operation
T_{encr}	time required by the system for executing encryption operation
T_{decr}	time required by the system for executing decryption operation
T_{exp}	time required for executing modulus exponential operation
$T_{pairings}$	time of executing a bilinear pairing operation

Table 2. The comparison of proposed identity based proxy signcryption scheme with the scheme in [21]

Algorithm	**The scheme in[6](with bilinear pairings)**	**The proposed scheme(without bilinear pairings)**
Proxy Key Generation	$4T_{EC\text{-}mult} + 2T_{EC\text{-}add} + 2T_{pairings} + 1T_{mult} + 2T_h$	$3T_{EC\text{-}mult} + 1T_{EC\text{-}add} + 5T_{mult} + 2T_h$
Proxy Signcryption	$2T_{EC\text{-}mult} + 1T_{EC\text{-}add} + 1T_{mult} + 2T_h + 1T_{pairings} +1\ T_{exp}+1\ T_{encr}$	$1T_{EC\text{-}mult} + 4T_{mult} + 1T_h +1\ T_{encr}$
Proxy Unsigncryption	$2T_{EC\text{-}mult} + 1T_{EC\text{-}add} + 3T_h + 3T_{pairings} + 1\ T_{decr}$	$3T_{EC\text{-}mult} + 1T_{EC\text{-}add} + 3\ T_{mult} + 2T_h +1\ T_{decr}$
Total	$8T_{EC\text{-}mult} + 2T_{EC\text{-}add} + 2T_{mult} + 7T_h + 6T_{pairings} + 1T_{exp}+ 1T_{encr} + 1T_{decr}$	$7T_{EC\text{-}mult} + 2T_{EC\text{-}add} + 12T_{mult} + 5T_h +1\ T_{encr}+1T_{decr}$

9. REFERENCES

[1] Y. Zheng. "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)", in Proc. Advances in Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, pp. 165-79, 1997.

[2] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization" Proceedings ofISW'00, pp. 308-322, 2000.

[3] B.H. Yum and P.J. Lee, "New signcryption schemes based on KCDSA" Proceedings of ICISC'01, LNCS 2288, pp. 305-317, Springer-Verlag, 2001.

[4] Y. Zheng, "Signcryption and its applications in efficient public key solutions," Proceedings of ISW'97, pp. 291-312, 1998.

[5] J. Baek, R. Steinfeld, and Y. Zheng. "Formal proofs for the security of signcryption", Journal of Cryptology, vol. 20, no 2, pp. 203-35, 2007.

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

[7] J. Malone-Lee, "Identity-Based Signcryption," Cryptology ePrint Archive, Report 2002/098, 2002.

[8] D. Boneh, and M. Franklin. "Identity-based encryption from the weil pairing", in Proc. Advances in Cryptology-CRYPTO 2001, LNCS 2139, Springer-Verlag, pp. 213-29, 2001.

[9] A. Fiat and A. Shamir, "How to Prove Yourself: Practical solutions to identification and signature problems," Proceedings of Crypto'86, LNCS 0263,pp. 186-194, Springer-Verlag, 1986.

[10] F. Hess, "Efficient identity-based signature schemes based on pairings," Proceedings of SAC 2002, LNCS2595, pp. 310-324, Springer-Verlag, 2002.

[11] F. Zhang, S. Liu, and K. Kim, "ID-Based One Round Authenticated Tripartite Key Agreement Protocol," Cryptology ePrint Archive, Report 2002/122, 2002.

[12] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bi- linear maps," Proceedings of Asiacrypt 2005, LNCS 3788, pp. 515-532, Springer-Verlag, 2005.

[13] X. Boyen, "Multipurpose identity-based Signcryption: A swiss army knife for identity-based cryptography," Proceedings of Crypto'2003, LNCS 2729, pp. 383-399, Springer-Verlag, 2003.

[14] L. Chen and J. Malone-Lee, "Improved Identity-Based Signcryption," Cryptology ePrint Archive, Report 2004/114, 2004.

[15] S. S.M. Chow, S.M. Yiu, L. C.K. Hui, and K.P.Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," Proceedings of ICISC 2003, LNCS 2971, pp. 352-369. Springer- Verlag, 2004.

[16] B. Libert and J.-J. Quisquater, "New identity-based signcryption schemes based on pairings," IEEE Information Theory Workshop, Paris, France, 2003.

[17] D. Nalla and K. C. Reddy, "Signcryption Scheme For Identity-based Cryptosystems," Cryptology ePrint Archive, Report 2003/066, 2003.

[18] R. Sakai and M. Kasahara, "Id-based cryptosystems with pairing on elliptic curve," Proceedings of Symposium on Cryptography and Information Security (SCIS'2003), 2003.

[19] F. Li, M.K. Khan, "A Survey of Identity-Based Signcryption," IETE Technical Review, Vol. 28, No. 3, pp. 265-272, 2011. (URL: http://www.tr.ietejournals.org/article.asp?issn=0256-4602;year=2011;volume=28;issue=3;spage=265;epage=272;aulast=Li)

[20] H. Chen, Yong Li, and Jinping Ren, " A Practical Identity-based Signcryption Scheme " , International Journal of Network Security, Vol.15, No.6, PP.484-489, Nov. 2013

[21] G. Swapna, P.V.S.S.N. Gopal, T. Gowri and P. Vasudeva Reddy," An Efficient ID-Based Proxy Signcryption Scheme", International Journal of Information & Network Security (IJINS) ,Vol.1, No.3, August 2012, pp. 200~206 ,ISSN: 2089-3299

[22] 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.

[23] H. M. Elkamchouchi , Eman F. Abu Elkhair and Yasmine Abouelseoud, "An Efficient Proxy Signcryption Scheme Based On The Discrete Logarithm Problem ", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013

[24] H. Lin , T. Wu and S. Huang " An Efficient Strong Designated Verifier Proxy Signature Scheme for Electronic Commerce" Journal Of Information Science And Engineering 28, 771-785 (2012)