An Efficient Identity-Based Proxy Signcryption for Secure Broadcast

Yeojeong Yoon†, Chanil Park†, Pyung Kim†, Seongoun Hwang‡, Hyunsoo Yoon†

† Network and Security Laboratory, Dept. of EECS, Div. of CS,
Korea Advanced Institute of Science and Technology,
373-1, Yuseong-Gu, Guseong-Dong, Daejeon 305-701, Republic of Korea
{yjyoon, chanil, pkim, hyoon}@nslab.kaist.ac.kr
‡Dept. of Computer and Information Communication Engineering,
Hongik University, Jochiwon, Yeongi, Chungnam, 339-701, Republic of Korea
sohwang@hongik.ac.kr

Abstract

To our best knowledge, no identity-based proxy broadcast signcryption scheme is known despite of the broadcast communication and the ability of delegation is widely used in many hierarchical ubiquitous computing groups. In this paper, we describe the first identity-based proxy broadcast signcryption scheme(IBPBSC). The proposed scheme supports the dynamic broadcast signcryption while achieving the security properties as well as providing the ability of delegating the signcrypting capacity from an original signcrypter to a proxy signcrypter. It is also very efficient in the aspect of communication because the size of ciphertexts and private keys in the scheme is constant, regardless of the size of receiver set. In addition, we analyze the proposed scheme from efficiency and security points of view.

1. Introduction

As the ubiquitous computing rapidly advances, the demand of the communication between a sender and a number of receivers increases considerably. Indeed, many ubiquitous computing application uses the broadcast communication rather than 1:1 communication that is significantly inefficient in the broadcast environment. Accordingly, it need an efficient Broadcast Encryption(BE) for the secure transaction in the ubiquitous network. The concept of BE was introduced by Fiat and Naor in [9]. In BE schemes, a broadcaster encrypts messages and transmits them to a group of privileged users who are listening to a broadcast channel. After receiving the broadcast message, privileged users use their private keys to decrypt transmissions. At encryption time, the broadcaster can choose a set S of identities that will be able to decrypt messages. A BE scheme is said to be fully collusion resistant when they can by no means infer information about the broadcast message even if all users that are not in S collude. Many BE systems have been proposed [5, 1, 13]. Specially, in [13], they introduced the concept of Dynamic Broadcast Encryption(DBE). A DBE scheme is a BE in which the total number of users is not fixed in the setup. Thus the DBE scheme is suitable for some applications, like DVD encryption. In 2007, Cécile proposed the first Identity-Based Broadcast Encryption(IBBE) with constant size ciphertexts and private keys in [11]. After that, Selvi et al. proposed a multi-receiver Identity-Based Signcryption scheme(m-IBSC) in [7] which efficiently combines a IBBE scheme with a signcryption. Signcryption, first proposed by Zheng[10], is a new cryptographic primitive which simultaneously fulfill both the functions of signature and encryption in a single logical step. Hence it reduces the computational cost significantly compared to the traditional signature-then-encryption approach.

In BE, we consider a scenario where an original sender wants to delegate the signcrypting capacity to a proxy sender and then the proxy sender can securely send a message to a dynamically changing subset of the receivers in such a way that non-members of this subset cannot learn the message. For example, suppose a president of a company has the capacity to signcrypt the important messages using the secret information and he needs to go on a business trip. During the trip, somebody must send the signcrypted messages to a large number of employees but the president doesn't want to reveal the secret information to anyone. To simply delegate the sign capacity, he can use proxy signature schemes[2, 3, 4, 8]. A proxy signature scheme enables a proxy signer to sign messages on behalf of the original signer. Upon receiving a proxy signa-

ture on some message, a verifier can validate its correctness through the given verification procedure, and then is convinced of the original signer's agreement on the signed message. Also there exist some identity-based proxy signcryption schemes[6, 14, 15, 16] which efficiently combines an identity-based proxy signature scheme with a signcryption. However, in this situation, the president needs a solution which is efficient in all three features : signcryption, delegation, and dynamic broadcast. Until now, there was no practical scheme which can be adapted to this scenario. Hence we propose a new scheme that achieves both confidentiality and authenticity simultaneously in this setting. In this paper, we describe the first identity-based proxy broadcast signcryption scheme(IBPBSC) and analyze the proposed scheme from efficiency and security points of view. The proposed scheme supports the dynamic broadcast as well as the delegation of the signcrypting power. It is also very efficient in the aspect of communication because the size of ciphertexts and private keys of the scheme is constant, regardless of the size of receiver set. The scheme is very useful in many applications, particularly in the broadcast communication environments of the ubiquitous computing where delegation of rights is quite common, such as mobile agents for electronic commerce, grid computing, global ubiquitous networks, and communication of hierarchical group like the military information environment.

The rest of this paper is organized as follows. Some definitions and preliminary works are given in Section 2. We also give the framework and the security requirements of identity-based proxy broadcast signcryption scheme in Section 2. Section 3 describes our identity-based proxy broadcast signcryption scheme. Section 4 analyzes the scheme and Section 5 presents our concluding remarks.

2. Preliminaries

Before describing the detail scheme, we briefly explain some notations and definitions.

2.1. Bilinear Pairing

Let $\mathbb{G}_1$ be an additive cyclic group of prime order p and $\mathbb{G}_2$ be a multiplicative cyclic group of the same order p.

A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties.

1) ***Bilinearity.*** For all $P, Q, R \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p^*$,

- $e(P + Q, R) = e(P, R)e(Q, R)$
- $e(P, Q + R) = e(P, Q)e(P, R)$
- $e(aP, bQ) = e(P, Q)^{ab}$

2) ***Non-Degeneracy.*** There exist $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq I_{G_2}$, where $I_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$

3) ***Computability.*** There exist an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

2.2. Framework of Identity-Based Proxy Broadcast Signcryption(IBPBSC)

An Identity-Based Proxy Broadcast Signcryption(IBPBSC) scheme for sending a single message to t users consists of the following five probabilistic polynomial time algorithms.

1) Setup(k,N) : Given a security parameter k and the size of the maximal set of receivers N, the Private Key Generator (PKG) generates the public parameters $params$ and master private key MSK of the system.
2) Extract(ID_i, MSK) : Given an identity ID_i, the PKG computes the corresponding private key S_i.
3) Generation of the proxy key(S_A) : To delegate the signcrypting capacity to a proxy signcrypter B, the original signcrypter A makes the signed warrant m_w and the proxy key U_A using the private key of A.
4) Proxy signcryption($m, m_w, ID_B, ID_1, ..., ID_t, S_B, U_A$) : To send a message m to receivers ($ID_1, ..., ID_t$), a proxy signcrypter B with identity ID_B runs this algorithm using the proxy key U_A and his private key S_B to obtain the signcryption σ of m.
5) Unsigncryption($\sigma, m_w, ID_A, ID_B, ID_i, S_i$) : When a user with identity ID_i and private key S_i receives a ciphertext σ, user ID_i runs this algorithm to obtain either the plaintext m or $\perp$ according as whether σ is a valid signcryption.

2.3. Security Requirements of Identity-Based Proxy Broadcast Signcryption

Because proxy signcryption is an integration of proxy signature and signcryption, we discuss a secure proxy signcryption scheme should satisfy the security requirements for proxy signature and signcryption simultaneously. Following the description from [6], an identity-based proxy broadcast signcryption scheme should satisfy the following five properties.

1) Verifiability: From the proxy signcryption, the recipient can be convinced of the original sender's agreement on the signcrypted message.
2) Strong unforgeability: The original sender and other third parties cannot create a valid proxy signcryption.
3) Strong identifiability: Anyone can determine the

identity of the corresponding proxy signcrypter from the proxy signcryption.
4) Prevention of misuse: The proxy signcrypter cannot use the proxy private key for other purposes than generating a valid proxy signcryption.
5) Confidentiality: Except the privileged recipients, any one cannot extract the plaintext from the ciphertext.
6) Non-repudiation: The recipient can efficiently prove to a third party that a message is indeed originated from a specific proxy signcrypter on behalf of an original sender.

3. Our proposed scheme

In this section, we proposed an identity-based proxy broadcast signcryption scheme. The scheme consists of the following five algorithms.

[Setup] Let λ be a security parameter of the scheme and N be the maximal size of the receiver set. $\mathbb{G}_1$, $\mathbb{G}_2$ are two groups of prime order p, where $|p| = \lambda$. P and Q are generators of $\mathbb{G}_1$ and e is a bilinear map defined as $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Let n_0,n_1, and n_2 denote the number of bits required to represent an identity, a message, and a warrant respectively. Four hash functions $H_1 : \{0,1\}^{n_0} \rightarrow \mathbb{Z}_p^*$, $H_2 : \{0,1\}^{n_1} \times \mathbb{G}_2 \rightarrow \mathbb{Z}_p^*$, $H_3 : \{0,1\}^{n_1+n_2} \times \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$, $H_4 : \mathbb{G}_2 \rightarrow \{0,1\}^{n_1+2|\mathbb{G}_1|}$ are used. The PKG chooses $s \in_R \mathbb{Z}_p^*$ and computes $R = sP$ and $g = e(P,Q)$.
The public parameters are
$params = \langle \mathbb{G}_1, \mathbb{G}_2, R, Q, sQ, s^2Q, ..., s^NQ, g, e(\cdot,\cdot), H_1, H_2, H_3, H_4 \rangle$.
The Master Secret Key is

$$MSK = \langle s, P \rangle.$$

[Extract] The private key of identity ID is

$$S_{ID} = \frac{1}{H_1(ID)+s} P.$$

[Generation of the proxy key] To delegate the signcrypting capacity to a proxy signcrypter B, the original signcrypter A does the following to make the signed warrant m_w. The warrant m_w includes an explicit description of the relative rights and information of the original signcrypter and proxy signcrypter. Thus a verifier can use it as a part of verification information. If the following process is finished successfully, the proxy signcrypter gets a proxy key U_A.

- A chooses r_A uniformly and randomly from $\mathbb{Z}_p^*$.
- A computes the following.
  1. $\alpha = g^{r_A}$
  2. $c_A = H_2(m_w, \alpha_A)$
  3. $U_A = (c_A + r_A)S_A$
- Original signcrypter A sends $\langle m_w, c_A, U_A \rangle$ to proxy signcrypter B without secure channel.
- Proxy signcrypter B verifies the validity of the proxy key.
  1. Compute $\alpha'_A = e(U_A, QH_1(ID_A) + sQ) \cdot g^{-c_A}$.
  2. Accept U_A if and only if $c_A = H_2(m_w, \alpha'_A)$.

  This step is done only once between the original signcrypter and the proxy signcrypter. Thus the proxy signcrypter needs to compute one pairing only once. If it is finished successfully, the proxy signcrypter can signcrypt any message which conforms to the warrant on behalf of the original signcrypter.

[Proxy Signcryption] Suppose proxy signcrypter B wants to send a message m to t receivers with identities $ID_1, ..., ID_t$. B does the following.

- Choose r_{p_1} and r_{p_2} uniformly and randomly from $\mathbb{Z}_p^*$.
- Compute the following.
  1. $r = r_{p_1} + c_A \cdot r_{p_2},\ \alpha_{A_P} = (\alpha_A)^{r_{p_2}}$
  2. $K = g^r \cdot \alpha_{A_P}$
  3. $X = -rR$
  4. $c_P = H_3(m_w||m, K)$
  5. $U_P = (c_P + r_{p1})S_P$
  6. $U'_A = r_{p_2}U_A$
  7. $c = m||U_P||U'_A \oplus H_4(K)$
  8. $y = [\prod_{i=1}^{t}(s + H_1(ID_i)]rQ$
- The signcryption is $\sigma = \langle c, X, y, m_w, \alpha_{A_P}, L \rangle$, where L is the list of receivers who can unsigncrypt σ.

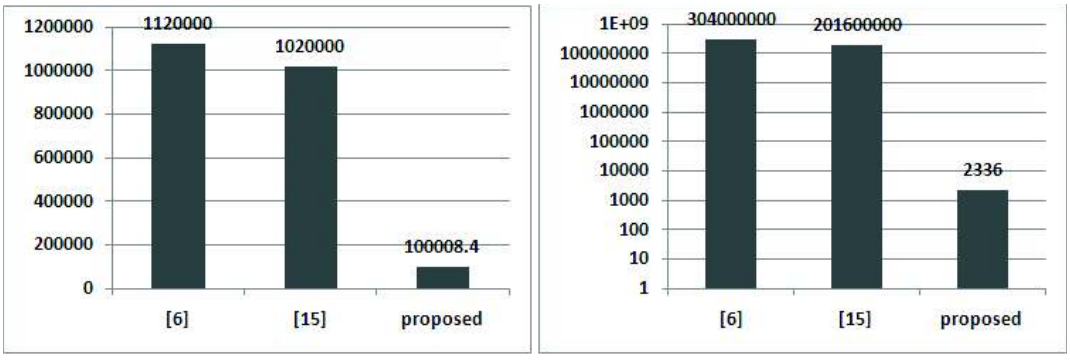
[Unsigncryption] A receiver with identity ID_i uses his private key S_i to unsigncrypt $\sigma = \langle c, X, y, m_w, \alpha_{A_P}, L \rangle$ as follows.

- Compute the following.
  1. $t_1 = \frac{1}{s}Q[\prod_{j=1,j\neq i}^{t}(s + H_1(ID_j)) - \prod_{j=1,j\neq i}^{t} H_1(ID_j)]$
  2. $t_2 = \frac{1}{\prod_{j=1,j\neq i}^{t} H_1(ID_j)}$
  3. $K' = [e(S_i, y) \cdot e(X, t_1)]^{t_2} \cdot \alpha_{A_P}$
  4. $m||U_P||U'_A = c \oplus H_4(K')$
  5. $c'_P = H_3(m_w||m, K')$
- If $K' = e(U_P, QH_1(ID_B) + sQ) \cdot e(U'_A, QH_1(ID_A) + sQ) \cdot g^{-c'_P}$, return m. Otherwise, return $\perp$.

Table 1. Comparison of computation and communication cost with a transmission from a sender to t receivers

	[6]	[15]	proposed
proxy generation	$3P + 2E + 4M$	$3P + 1E + 3M$	$1P + 2E + 3M$
proxy signcryption	$2tP + 2tE + 2tM$	$2tP + 2tE + tM$	$2E + (5 + t)M$
unsigncryption	$3P + 3E + 2M$	$8P + 2E + 9M$	$4P + 2E + (2t + 5)M$
communication	$n_1t + 2n_2t + 2t\lvert\mathbb{G}\rvert + t\lvert\mathbb{Z}_p^*\rvert$	$n_1t + n_2t + 2t\lvert\mathbb{G}\rvert + t\lvert\mathbb{Z}_p^*\rvert$	$n_1 + n_2 + 5\lvert\mathbb{G}\rvert$

P : pairing in $\mathbb{G}$, E : exponentiation in $\mathbb{G}$, M : multiplication in $\mathbb{G}$, A : addition in $\mathbb{G}$, t : the number of receivers
n_0, n_1, and n_2 denote the number of bits required to represent an identity, a message, and a warrant respectively.



(a) computation for the proxy signcryption (unit : ms)

(b) communication cost (unit : bits) (Note : The vertical axis uses logarithmic scale.)

Figure 1. Comparison of computation and communication cost with $t = 10^6$

4. Analysis of proposed scheme

4.1. Correctness

It is easy to see that the unsigncryption algorithm of our scheme is consistent. Indeed, if σ is a valid ciphertext to ID_i,

$$
\begin{aligned}
e(S_i, y) &= e(P, Q)^{r[\prod_{j=1, j\neq i}^{t}(s+H_1(ID_j))]} \\
e(X, t_1) &= e(P, Q)^{-r[\prod_{j=1, j\neq i}^{t}(s+H_1(ID_j)) - \prod_{j=1, j\neq i}^{t} H_1(ID_j)]} \\
\beta &= e(S_i, y) \cdot e(X, t_1) \\
&= e(P, Q)^{\prod_{j=1, j\neq i}^{t} H_1(ID_j)} \\
&= g^{r \cdot \prod_{j=1, j\neq i}^{t} H_1(ID_j)}
\end{aligned}
$$

$Hence,$

$$
\begin{aligned}
K &= \beta^{\frac{1}{\prod_{j=1, j\neq i}^{t} H_1(ID_j)}} \cdot \alpha_{A_P} \\
&= \beta^{t_2} \cdot \alpha_{A_P}.
\end{aligned}
$$

4.2. Efficiency

Now we describe about the efficiency of the proposed identity-based proxy broadcast signcryption scheme. Suppose that the proxy signcrypter B wants to send a message to t receivers using existing identity-based proxy signcryption scheme that is not broadcast scheme, then B needs t ciphertexts corresponding to each of the receivers. However, if B uses the proposed scheme, then he needs just one ciphertext to send the message to t receivers. Thus it is obvious the proposed scheme is more efficient in terms of computation and communication cost than existing identity-based proxy signcryption schemes in the broadcast environment.

To show the strict efficiency comparison, it need to compare the efficiency of our IBPBSC with other IBPBSC. However, to our knowledge, there is no IBPBSC known until now. Hence, we suppose that the proxy signcrypter B sends the message to t receivers using the existing identity-based proxy signcryption schemes [6, 15]. In Table 1, we enumerate the various operations necessary for each and the communication cost. For convenience of comparison, we denote $\mathbb{G}_1 = \mathbb{G}_2$ by $\mathbb{G}$. Since the schemes in [6, 15] are 1:1 communication scheme between a proxy signcrypter and a receiver, it requires to execute t proxy signcryption algorithm in the broadcast communication. Thus [6] and [15] require $2tP + 2tE + 2tM$ and $2tP + 2tE + tM$ in proxy signcryption algorithm to make t ciphertexts, respectively. In the other word, all computation required for proxy

signcryption is linear in the number of receivers. However, we require just $2E + (5 + t)M$ computations since it needs just one ciphertext to broadcast a message to t receivers. Indeed, only the number of multiplication is linear in t. But we note that the computation of pairing operations is the most time-consuming and multiplication operations need smaller computations than pairing and exponentiation operations. Thus the proposed scheme is much more efficient than [6, 15] because no pairing is needed in proxy signcryption algorithm. Furthermore, in [6] and [15], they use the additional ideal symmetric key encryption/decryption algorithms $E_K(\cdot)/D_K(\cdot)$. Thus they need extra computations for encryption and decryption while we can encrypt and decrypt using just above computation. Also, in terms of communication cost, [6] and [15] require $n_1t + 2n_2t + 2t|\mathbb{G}| + t|\mathbb{Z}_p^*|$ and $n_1t + n_2t + 2t|\mathbb{G}| + t|\mathbb{Z}_p^*|$ respectively to transmit the t ciphertexts to each t receivers because the schemes are not broadcast ones. However the proposed scheme requires much smaller communication cost, $n_1 + n_2 + 5|\mathbb{G}|$, because it needs constant size ciphertexts to broadcast.

Fig. 1 is the simulation result to verify the practical efficiency of the proposed scheme using the Pairing-Based Cryptography Library(PBC)[12]. We set a prime $p \approx 2^{512}$, $|\mathbb{Z}_p^*| = 512$, $|\mathbb{G}| = 160$, $|ID|$ = 160, and the number of receivers $t = 10^6$. We also get the following operation times using the PBC library[12] on a 3.0 GHz Pentium D desktop machine : pairing in $\mathbb{G}$ = 2.0ms, exponentiation in $\mathbb{G}$ = 1.7ms, multiplication in $\mathbb{G}$ = 1.0ms. We used logarithmic scale of measured data on the vertical axes of the figure (b) in Fig. 1, because the cost of [6, 15] is so high that we could not present the cost of the proposed scheme same figure. Fig. 1 shows that the computation overhead and communication cost of the proposed scheme is significantly lower than those in the other schemes. Especially, we can see the tremendous difference in communication cost between [6, 15] and the proposed scheme with figure (b) in Fig. 1. The result is reasonable because the ciphertexts of the proposed scheme is constant while those in the other schemes grow linear in the size of the set of receivers. Therefore we can conclude that the proposed scheme is very useful in large scaled broadcast environment.

In addition, we note that the proxy signcrypter has to send the set L of identities that are included in the ciphertext. This set is needed to unsigncrypt, as in previous schemes, thus it is counted in the full header, but not in the header. Therefore, as we said before, the ciphertexts of the scheme is constant.

4.3. Security

We show that the proposed identity-based proxy broadcast signcryption scheme satisfies all the security requirements stated in Section 2.3.

1) Verifiability: From the proxy unsigncryption phase, the receiver can be convinced that the proxy signcrypter has the original signcrypter's signature on the warrant m_w. Since the warrant m_w also contains the identity information and the limit of the delegated signcrypting capacity, the receiver can verify the original signcrypter's agreement on the signcrypted message. Thus the scheme satisfies the verifiability.

2) Strong unforgeability: The adversary who wants to forge the proxy signcryption of the message m' must have the original signcrypter's signature c'_A and U'_A on a modified warrant m'_w. To compute $U'_A = (c'_A + r'_A)S_A$, the adversary has to obtain the original signcrypter's private key S_A. However, the attacker cannot get the value $S_A = \frac{1}{H_1(ID_A)+s}P$ because s, P are the Master Secret Key. Thus the adversary doesn't able to forge this signature. On the other hand, the original signcrypter cannot create a valid proxy signcryption since $U_P = (c_P + r_{p1})S_P$ includes the private key S_P of the proxy signcrypter. Therefore the scheme satisfies the strong unforgeability. In addition, since the proxy signcryption step of the proposed scheme is based on [7], it is straightforward to show that our scheme is existentially unforgeable under chosen message attack under the l-Strong Diffie-Hellman Problem(l-SDHP) assumption similar to [7].

3) Strong identifiability: The proposed scheme contains the warrant m_w in a valid proxy signcryption, and anyone can determine the identity of the corresponding proxy sender from the warrant m_w. Thus the scheme satisfies the strong-identifiability.

4) Prevention of misuse: In our scheme, using the warrant m_w, we have determined the limit of the delegated signcrypting capacity. Hence the proxy signcrypter cannot signcrypt messages that have not been authorized by the original signcrypter. Thus the scheme satisfies the prevention of misuse.

5) Confidentiality: Except the privileged receiver, anyone else cannot extract the plaintext m from the ciphertext $\sigma = \langle c, X, y, m_w, \alpha_{A_P}, L\rangle$. For getting the message, the attacker has to decrypt the ciphertext σ directly. To do so, the attacker has to know the $K = [e(S_i, y) \cdot e(X, t_1)]^{t_2} \cdot \alpha_{A_P}$. However, the attacker doesn't able to get the value $S_i = \frac{1}{H_1(ID_i)+s}P$ because s, P are the Master Secret Key. Thus the scheme satisfies the confidentiality. In addition, since the proxy signcryption step of the proposed scheme is based on [7], it is straightforward to show that our scheme is semantically secure against chosen ciphertext attacks under the General Decision Diffie-Hellman Exponent(GDDHE) assumption similar to [7].

6) Non-repudiation: As the strong-identifiability, the valid proxy signcryption contains the warrant m_w, which

must be used verification phase. Hence it cannot be modified by the proxy signcrypter. Therefore once a proxy signcrypter creates a valid proxy signcryption of an original signcrypter, he doesn't able to repudiate the signcryption creation.

5. Conclusion

Lately, the broadcast communication and the ability of delegation is widely used in many hierarchical ubiquitous computing groups. Although there exist some identity-based proxy signcryption schemes[14, 15, 6, 16], to our best knowledge, no identity-based proxy broadcast signcryption is known. Hence, we introduced the first identity-based proxy broadcast signcryption scheme(IBPBSC). The proposed scheme has desirable properties such as dynamic broadcast, proxy signature, and signcryption, but with a better efficiency in large scaled broadcast environment. In addition, we analyzed the proposed scheme from efficiency and security points of view. For the future work, we plan to involve the security proof of our scheme.

Acknowledgment

This research is supported by the Ubiquitous Computing and Network(UCN) Project, Knowledge and Economy Frontier R&D Program of the Ministry of Knowledge Economy(MKE) in Korea as a result of UCNs subproject 10C1-T1-20S.

References

[1] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, CRYPTO 2005, volume 3621 of LNCS, Springer-Verlag, Berlin, Germany, pp.258-275, Santa Barbara, CA, USA, August 14.18, 2005.

[2] M.Mambo,K.Usuda,E.okamoto. Proxy signature: delegation of the power to sign messages. IEICE Trans.Fundamentals. E79-A:9, pp.1338-1353, 1996.

[3] S. Kim, S. Park, and D. Won, Proxy signatures, revisited, In Pro. of ICICS 97, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.

[4] B. Lee, H. Kim and K. Kim. Secure mobile agent using strong non-designated proxy signature. Proc. of ACISP2001, LNCS 2119, pp.474-486, Springer Verlag, 2001.

[5] Dani Halevy and Adi Shamir. The LSD broadcast encryption scheme. In MotiYung, editor, CRYPTO 2002, volume 2442 of LNCS, Springer-Verlag, Berlin, Germany, pp.47-60, Santa Barbara, CA, USA, August 18.22, 2002.

[6] Q. Wang and Z. Cao. Two proxy signcryption schemes from bilinear pairings. Proc of CANS 2005, Berlin: Springer-Verlag, LNCS 3810, pp.161-171, 2005.

[7] S. S D Selvi,S. S Vivek,R. Srinivasan, et al. An efficient identity-based signcryption scheme for multiple receivers. In: Advances in Information and Computer Security 2009, LNCS Vol. 5824. Berlin: Springer-Verlag, pp.71-88, 2009.

[8] T. Okamoto, M. Tada and E. Okamoto. Extended proxy signatures for smart cards. ISW99, LNCS 1729,Springer-Verlag, pp.247-258, 1999.

[9] Amos Fiat and Moni Naor. Broadcast encryption. In Douglas R. Stinson, editor, CRYPTO93, volume 773 of LNCS, Springer-Verlag, Berlin, Germany, pp.480.491, Santa Barbara, CA, USA, August 22.26, 1994.

[10] Yuliang Zheng. Digital Signcryption or How to Achieve Cost (Signature & encryption) << Cost (Signature) + Cost (Encryption). CRYPTO 1997, Lecture Notes in Computer Science, Vol.1294, pp.165-179, Springer-Verlag, 1997.

[11] Cécile Delerablée. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In ASIACRYPT 07, pp.200-215, 2007.

[12] The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/.

[13] Cécile Delerablée, Pascal Paillier, and David Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In T. Takagi et al., editor, PAIRING 2007, volume 4575 of LNCS, Springer-Verlag, Berlin, Germany, pp.39-59, 2007.

[14] Xiangxue Li and Kefei Chen. Identity Based Proxy-Signcryption Scheme from Pairings. In IEEE SCC, pp.494-497, 2004.

[15] M Wang, H Li, Z Liu. Efficient Identity Based Proxy-Signcryption Schemes with Forward Security and Public Verifiability. Networking and Mobile Computing, Springer Berlin/Heidelberg, pp.982-991, 2005.

[16] Hassan Elkamchouchi and Yasmine Abouelseoud. A New Proxy Identity-Based Signcryption Scheme for Partial Delegation of Signing Rights. ACR ePrint Archive, http://eprint.iacr.org/2008/041.pdf, 2008.

