Vol.2016-DPS-166 No.31
Vol.2016-CSEC-72 No.31
2016/3/4

An Examination of A Secure Multicast Scheme Based on User-centric IBE

EI KHAING WIN[†1] TOMOYA KAWAKAMI[†3] YOSHIMASA ISHI[†1]
TOMOKI YOSHIHISA[†1] YUUICHI TERANISHI[†1,2] SHINJI SHIMOJO[†1]

Abstract: In this paper, we propose an efficient and secure multicast scheme, in which a sender can disseminate, an encrypted message to the receivers using identity-based encryption scheme (IBE), which has become a prevalent scheme of the public key encryption for secure data exchanges. As an encryption method for multi-recipient data disseminations, various identity-based encryption schemes have been proposed. However, existing schemes assume to generate keys on the sender. In dynamic environments, a large number of users (data owners) will join and/or leave simultaneously. As a result, there can be excessive computation loads for key generation on the sender. Our proposal applies a user-centric IBE scheme to the multicast encryption to reduce key generation loads of the senders and presents new multicast scheme. We have implemented a prototype of our scheme and evaluated its performances.

Keywords: multicast scheme, identity-based encryption, multi-recipient data dissemination, user-centric IBE

1. Introduction

Due to the advances in cyber physical systems, the importance of ad-hoc secure group communication services is increasing. The ad-hoc secure group communication includes delivering privileged notifications or sensor information for people/vehicles only in a certain situation such as in a bad health status, in a shopping mall, on a road, etc. Such information services need to realize secure multicast. Instead of sending data to each recipient, multicast allows sender to send a message just one time for all recipients. Multicasting is the popular scheme that requires the sender to send the same message to a large set of receivers only once. In comparison with unicast, where the sender has to send the same message to each receiver individually, multicasting reduces the overhead of sender. To keep the message confidential, only the privileged receivers need to be able to decrypt the received message. The receiver also needs to authenticate message sender so that the information is created by a trusted entity. Examples can be described for personalized services and decentralized systems. Depending on required services, user (data owner) has to decide data receivers (service providers) by themselves to control data access directly. In that case, source authentication is very important to ensure secure result came from authenticated senders (service providers). As secure multicast schemes, IBE-based encryption schemes recently attract attention because they require less key management costs for group communication [1, 2, 3, 4, 5, 6, 7]. However in these existing IBE-based schemes, key generation centers (KGCs) need to generate private keys for all receivers and senders. However, key generation of IBE-based scheme requires high computation load. Therefore, if a massive number of receivers newly requests to receive encrypted messages from a sender, the corresponding KGC falls into heavy CPU load, which may induce the long latency for multicast message delivery. In this paper, we propose secure multicast scheme using broadcast encryption system based on user-centric IBE scheme to cope with this problem.

2. Related Works

The concept of Identity-based broadcast encryption was introduced in [9]. In [7], efficient identity-based multi-receiver broadcast encryption has been proposed. Instead of n times encryptions using Boneh and Franklin's identity-based encryption, the scheme only needs one pairing computation to encrypt a single message for n receivers. In [10], authors propose the dynamic broadcast encryption system to improve all efficiency measures for time and size of private key. Many schemes such as [5, 11, 12] have also been proposed for achieving identity-based broadcast encryption schemes with short ciphertexts and private keys size for receivers, collusion resistance, short constant length private keys, and public key proportional to the number of receivers, according to different property.

In [6], an efficient dynamic identity-based broadcast encryption scheme (DIBBE) was presented and compared with Delerablee's identity-based encryption. The security of scheme is also proved in the Random Oracle model. Another efficient identity-based broadcast encryption system without Random Oracle has been proposed in [13].

Until now, existing IBBE schemes consist of key extraction stage or key setup stage on sender to generate private keys for users (data owners). By using that private key, user can send its data to sender and sender can reply to user (one-to-one communication). Moreover, users (data owners) use that private key to decrypt broadcast message for n users (data owners) encrypted by sender using only one pairing computation instead of n time encryptions (one-to-many communication). This can be achieved as only sender generates private keys for all users (data owners). In case of users (data owners) generating private keys for their desired parties, although reducing load of sender, there exists no scheme for broadcast. In this paper, we will develop a prototype of user-centric IBE based broadcast scheme

†1 Osaka University
†2 National Institute of Information and Communications Technology
†3 Nara Institute of Science and Technology

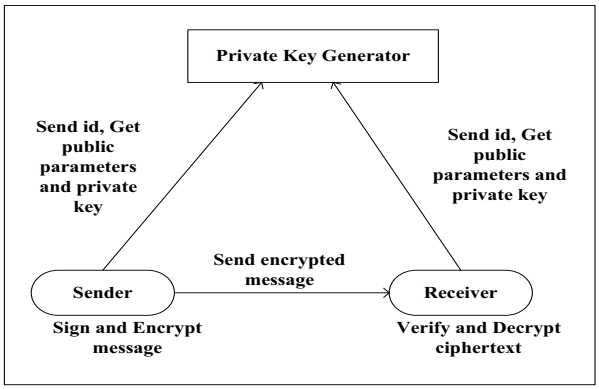

Figure 1: Identity-based Encryption

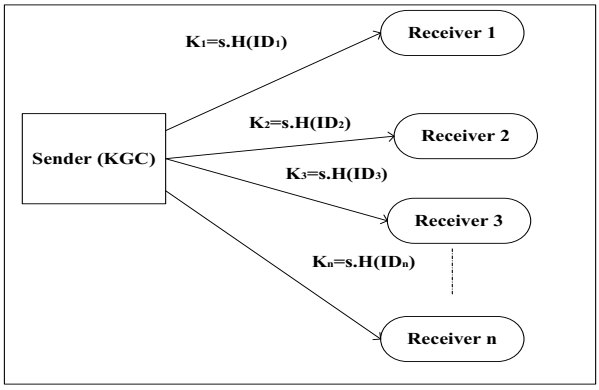

Figure 2: Private Key Extraction on IBE

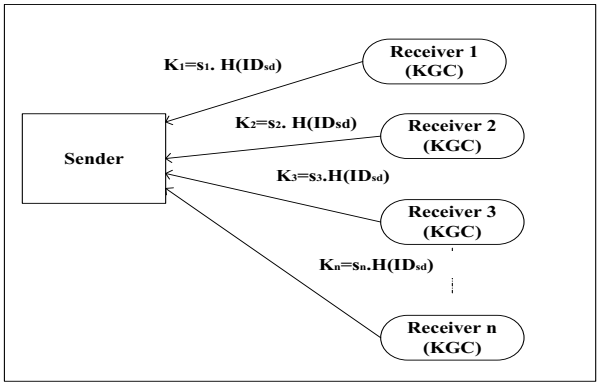

Figure 3: Private key Extraction on Uc-IBE

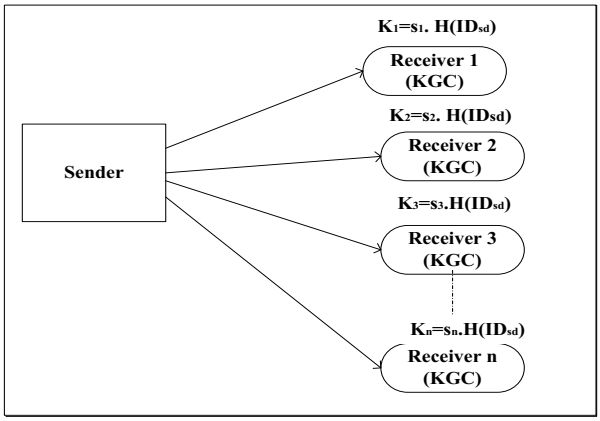

Figure 4: User-centric IBE based Broadcast Encryption

and evaluate its performances in comparison with IBBE scheme [6] and comparison schemes.

3. Assumptions

3.1 Bilinear Maps

Let G_1, G_2 be two additive cyclic groups of prime order q, and GT be another cyclic group of order q. A pairing is a map $e: G_1 \times G_2 \rightarrow GT$, which satisfies the following properties:

- Bilinearity
  $\forall a, b \in F_q^*, \forall P \in G_1, Q \in G_2: e(aP, bQ) = e(P, Q)^{ab}$
- Non-degeneracy: $e(P, Q) \neq 1$
- Computability: there exists an efficient algorithm to compute e [14]

A bilinear map satisfying the three properties above is said to be an admissible bilinear map.

3.2 Identity-based Encryption

Identity based encryption (IBE), in Figure 1, introduced by Shamir [15], uses unique string (e.g. an e-mail address, a telephone number, ip address etc.) as public keys. IBE scheme eliminates the need for certificates as used in a traditional public key infrastructure. Therefore, IBE scheme is more lightweight than public key infrastructure. Boneh and Franklin [16] presented the first practical IBE system (BF-IBE) based on groups with efficiently computable pairings. As shown in Figure 2, a private key generator (PKG) on sender computes private keys (K_1, K_2... K_n) (for user 1, user 2... user n) from a master secret (s) and distributes these to the entities participating in the scheme.

Then, the user who wants to send secure message must first sign the message, encrypt using destination identity, public parameters and send the ciphertext. Recipient must verify the message and then decrypt to get the plaintext.

3.3 User-centric IBE based Encryption (Uc-IBE)

According to ID-based encryption concept, Key Generation Center (KGC) is responsible for generation of users' (data owners') private keys. As a result, the sender may have excessive workload for key generation as the number of user increases and also for key revocation. In contrast to sender-centric IBE system, by shifting the workload (key generation) of sender to receiver side, instead of sender generating keys for all users (data owners), user-centric IBE system will reduce the workload of sender. In other words, it is user-level PKGs. It is illustrated in Figure 3 in which the receiver generates private key for sender (IDsd). In [17], data owner always generate keys for valid data receivers to take advantage for online social network in decentralized form. In [18], users (data owners) generate keys by themselves to allow data access to data receivers. Therefore, user-centric IBE scheme is suitable for applications in which user controls his own data access directly.

3.4 Identity-based Broadcast Encryption

Identity-based broadcast encryption is based on identity-based cryptography in which public keys are unique identities of the users (data owners). Instead of n time communications for n

receivers, broadcast encryption reduces overhead by sending the same ciphertext message to *n*-receivers by sending just one time.

An identity-based broadcast encryption scheme consists of four algorithms [6]: Set up, Extract, Encryption, and Decryption. Three algorithms: Set up, Extract and Encryption are performed on sender's side and receiver only performs Decryption algorithm

Setup (λ). Given the security parameter λ, a bilinear map group system B= (p, G1, G2, GT, e (,)) is constructed such that |p|=λ. Also, two generators$g \in G1\ and\ h \in G2$, are randomly selected as well as a secret value $\gamma \longleftarrow Zp$.Choose a cryptographic hash function $H: \{0,1\}^* \longrightarrow Z_p^*$. B and H constitute system public parameters. The master secret key is defined as MSK= (g, γ). The public key is PK = (v, h) where v = e (g, h).

Extract (MSK, ID). Given MSK = (g, γ) and the identity ID, it outputs $SK_{ID} = g^{1/\gamma.H(ID)}$

Encrypt (S, MSK, PK). Assume for notational simplicity that$S = \{ID_j\}_{j=1}^{s}$. Given PK= (v, h), the broadcaster randomly picks $k.r \longleftarrow Zp$.and computes Hdr = (T1, T2, C1, C2) and K where

$$T1 = r.\gamma^s \ mod\ p \quad , \quad T2 = \prod_{i=1}^{s} (H(ID_i))\ mod\ p$$

$$C1 = g^{-k/r} \qquad C2 = h^{k.\gamma.T1.T2/r} \qquad K = v^{k/r}$$

Encrypt outputs (Hdr,K). (Then K is used to encrypt the message)

Decrypt (S, IDi, sk, Hdr, PK). In order to retrieve the message encryption key K encapsulated in the header Hdr= (T1, T2, C1, C2), user with identity IDi and the corresponding private key $SK_{ID} = g^{1/\gamma.H(ID)}$, computes

$$P_{i,s}(\gamma) = \frac{(T1-1)T2}{H(IDi)}\ mod\ p$$

$$= \frac{(r.\gamma^s - 1)}{H(IDi)} \prod_{i=1}^{s} (H(ID_i))\ mod\ p$$

$$= (r.\gamma^s - 1) \prod_{i=1, i\neq j}^{s} (H(ID_i))\ mod\ p$$

Decryption is done using $[e(C1, h^{P_{i,s}(\gamma)}) e(SK_{ID}, C2)]^{\frac{H(IDi)}{T2}}$

$$\left[e\left(C1, h^{P_{i,s}(\gamma)}\right) e(SK_{ID}, C2)\right] = e(g,h)^{\frac{k}{r} \prod_{i=1,i\neq j}^{s} (H(ID_i)) . \frac{H(IDi)}{T2}.}$$

$$= e(g,h)^{\frac{k}{r}.}$$

Where

$$e\left(C1, h^{P_{i,s}(\gamma)}\right) = [e\left(g^{-k}, h^{(\gamma^s - 1/r) \prod_{i=1,i\neq j}^{s} (H(ID_i))\ mod\ p}\right))]$$

$$e\left((SK_{ID}, C2)\right) = \left[e\left(g^{1/\gamma.H(ID)}, h^{k.\gamma.T1.\frac{T2}{r}}\right)\right]$$

4. User-centric IBE based Broadcast Encryption

In this section, we propose a novel secure multicast method, which is based on the user-centric IBE. According to Figure 6, our scheme requires larger extraction time on receiver than comparison schemes. That extraction time will be proportional to the number of senders (Servers) and possibility for using large group of sender is less in this scenario. Another point is that the sender's encryption time will be better in our scheme for large groups of receivers.

4.1 Overview

In user-centric IBE scheme, each user has its own secret key (s_1, s_2, s_3, s_n) and generates corresponding decryption keys ($s_1H1(ID_1)$,$s_2H1(ID_2)$,..,$s_nH1(ID_n)$) for (IDsd) as shown in Figure 4. As all users and server possess different keys, broadcast message encrypted by server 's secret key (s), it is impossible for users to decrypt message by using his or her own decryption keys. To decrypt using own decryption key, server must do (*n*) times pairings for (*n*) users. Just one time encryption for intended group of users and multicast would reduce complexity. To achieve this, user-centric identity-based broadcast encryption scheme is proposed.

4.2 Formal Definition

Hereafter, we will describe our scheme formally.

- Set up (Sender) Choose $P \in G1, Q \in G2,\ \gamma \longleftarrow Zp,$ $H: \{0,1\}^n \longrightarrow G1, H1: \{0,1\}^n \longrightarrow Zp, H2: \{0,1\}^* \longrightarrow Zp$

$$Pub_s = (\frac{1}{\gamma}.P, \mathrm{Q})$$

$$MSK_s = (\gamma, \gamma.H(IDs))$$

- Encryption (Sender) Choose $m, n, k \longleftarrow Zp$

$$T1 = m. \prod_{i=1}^{t} H1(SK_{ID_i})$$

$$T2 = (\gamma^m.m^2 + m.n) \prod_{i=1}^{t} H1(SK_{ID_i})$$

$$C1 = P^{\frac{k}{m}}$$

$$C2 = Q^{-\gamma.k.T1.n/m}$$

$$K = e(P,Q)^{k.\gamma^m}$$

Where i=1, 2, 3…t and t=number of receivers

(Then K is used to encrypt the message)

$$C3 = E_K(Msg)$$

- Set up (Receiver) Choose $R \in G1, V \in G2,\ s\ \in Zp$

$$Pub_c = (R, \frac{1}{s}\mathrm{V})$$

$$MSK_c = s$$

- Extraction (Receiver)

$$x \leftarrow \{0,1\}^n$$

$$SK_{ID_i} = R^{1/s.H1(ID_i)}$$

$$BK_{ID_i} = \frac{1}{H1\left(SK_{ID_i}, x_i\right)}.Pub_s = \frac{1}{\gamma.H1\left(SK_{ID_i}, x_i\right)}P$$

- Decryption (Receiver)

$$[e(C1, h^U) e(BK_{ID_i}, C2)]^{\frac{H1\left(SK_{ID_i}, x_i\right)}{T1}}$$

First, calculate U.

$$U = \frac{T2}{H1(SK_{ID_i}, x)} = \frac{(\gamma^m.m^2 + m.n) \prod_{i=1}^{t} H1\left(SK_{ID_i}, x_i\right)}{H1(SK_{ID_i}, x)}$$

$$= (\gamma^m.m^2 + m.n) \prod_{j=1, i\neq j}^{t} H1(SK_{ID_j}, x_j)$$

- Correctness

$$[e(C1, h^U) e(BK_{ID_i}, C2)]^{\frac{H1\left(SK_{ID_i}, x_i\right)}{T1}}$$

$$e(C1, h^U) = e\left(P\frac{k}{m}, Q^{(\gamma^m.m^2+m.n)\prod_{j=1,i\neq j}^{t} H1\left(SK_{ID_j}, x_j\right)}\right)$$

$$= e(P,Q)^{\frac{k}{m}.\left[m(\gamma^m m+n)\prod_{j=1,i\neq j}^{t} H1\left(SK_{ID_j}, x_j\right)\right]}$$

$$= e(P,Q)^{k.\left[(\gamma^m m+n)\prod_{j=1,i\neq j}^{t} H1\left(SK_{ID_j}, x_j\right)\right]}$$

$e\left(BK_{ID_i}, C2\right)$=e $\left(\frac{1}{\gamma.H1\left(SK_{ID_i}, x_i\right)}P, Q^{-\gamma.k.T1.n/m}\right)$

$$=e(P,Q)^{\frac{1}{\gamma.H1\left(SK_{ID_i}, x_i\right)}.\left(-\gamma.k.T1.\frac{n}{m}\right)}$$

$$=e\ (P,Q)^{(-k.n)\prod_{j=1,i\neq j}^{t} H1\left(SK_{ID_j}, x_j\right)}$$

$$\left[e(C1, Q^U)e\left(BK_{ID_i}, C2\right)\right]^{\frac{H1\left(SK_{ID_i}, x_i\right)}{T1}}$$

$$= \left[e(P,Q)^{k.\gamma^m m\left[\prod_{j=1,i\neq j}^{t} H1\left(SK_{ID_j}, x_j\right)\right]}\right]^{\frac{H1\left(SK_{ID_i}, x_i\right)}{m.\prod_{i=1}^{t} H1\left(SK_{ID_i}, x_i\right)}}$$

$$= e(P,Q)^{k.\gamma^m}$$

❖ Authentication and Integrity

Sign on Sender: Choose $w \in Zp$, IDs =identity of sender

$$s1 = \gamma^2.w$$

$$s2 = H2(C3, T1, T2, C1, C2)$$

$$s3 = s1 \oplus s2$$

$$s4 = e(s2.P, MSK_s)^w = e(s2.P, \gamma.H(IDs))^w$$

$$= e(P, H(IDs))^{\gamma.w.s2}$$

Sender sends (s3, s4) to recipients as signature.

Verify on Receiver:

$$cv = H2(C3, T1, T2, C1, C2)$$

$$s1 = s3 \oplus cv$$

$e(s1.cv.H(IDs), Pub_s) = e(H(IDs), P)^{r.w.cv}$.

4.3 Security Analysis

Assumption: Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve over a finite field (K). Suppose there are points $P, Q \in E(K)$ given such that$Q \in < P >$. Determine k such that$Q = [k]P$.

In our scheme, according to elliptic curve discrete logarithm problem, it is hard for adversary to get the broadcast key of others. Naïve brute force calculation for discrete logarithm problem will introduce complexity.

In our scheme, the source authentication scheme is added. The sender signs the encrypted message (C3), and broadcast parameters (T1, T2, C1, C2) by using its secret key ($\gamma.H(IDs)$). Receivers can verify the signature using sender identity (IDs), and sender's public key. Message integrity is also maintained together with authentication scheme. If the receiver's (cv) value and sender's (s2) value are not equal, then result will be different from sender's (s4) value. As a result, receiver can easily know that the sender's message has been altered. If verification process succeeds, then the receiver can decrypt the ciphertext. As users (data owners) control data access directly, users (data owners) can deliver their data to intended, multiple receivers for several actions. Only intended users (data owners) have accessible permission. Users (data owners) can dynamically change the group of intended receivers, time allowed for data access, and revocation to unintended receivers.

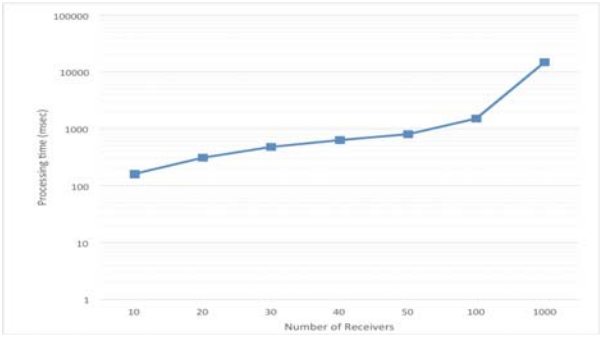

Figure 5: Extraction Time on Sender for IBE

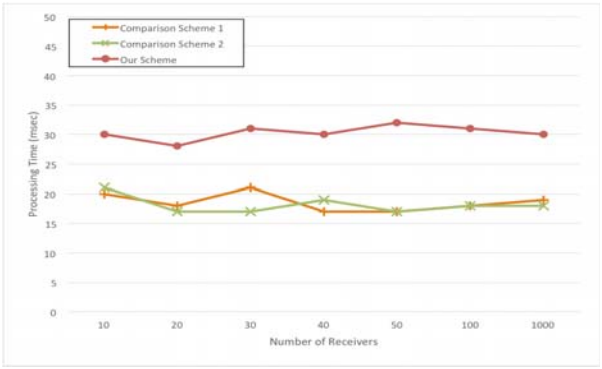

Figure 6: Key Extraction Time on Receiver for Uc-IBE

5. Performance Evaluation

In this section, we describe two comparison schemes based on user-centric IBE. The performance comparison of proposed scheme, comparison schemes and identity-based broadcast encryption scheme [6] are shown in Table 1 and 2. In comparison scheme (1), users (data owners) have different system parameters. For *n*-receivers, sender has to make (*n*) times, different pairings for encryption using (n) different system parameters. As a result, broadcast encryption time, parameter storage and ciphertext length linearly increases with the number of receivers. In comparison scheme (2) and our scheme, to make sender enable just one time pairing encryption, users (data owners) use the same system parameters declared by the sender. In this way, sender's broadcast encryption time is reduced for large set of receivers. Scheme (2) will enable receivers to decrypt message using only own-generated private keys (no extra private key from sender). Sender's system parameter storage will be less than comparison scheme (1) and no need to generate *n* broadcast private. However, comparison scheme (2) has *n*-size ciphertext length. To get constant ciphertext length and better encryption time, our scheme encrypts message using symmetric key.

Efficiency is measured in terms of public key length, private key length, pairing operations, ciphertext length, public parameter storage on sender, encryption time, and overall load on sender. Also key extraction time comparison is shown in Figure 5 and 6 respectively. Decryption time on receiver is also illustrated in Figure 9.

5.1 Comparison Scheme 1

Sender has to use different system parameters for different

users (data owners), $H:\{0,1\}^* \longrightarrow G1$, $H1: G1 \longrightarrow \{0,1\}^*$, Msg$\longrightarrow$ $\{0,1\}^*$

- Encryption (Sender) Choose $\gamma \longleftarrow Zp$

$$C = \gamma . R$$

$$T_i = Msg \oplus H1\left(e\left(H\left(ID_i\right), Pub_{c_i}\right)^{\gamma}\right)$$

Where i=1, 2, 3…t

t=number of receivers

- Set up (Receiver) Choose $R \in G1, V \in G2,\ s \in Zp$

$$Pub_c = sR, R$$

$$MSK_c = s$$

- Extraction (Receiver)

$$SK_{ID_i} = s.H(ID_i)$$

- Decryption (Receiver)

$$T_i \oplus e(SK_{ID_i}, C)$$

- Correctness

$$T_i \oplus H1\left(e(SK_{ID_i}, C)\right)$$

$= Msg \oplus H1\left(e\left(H\left(ID_i\right)_i, Pub_{c_i}\right)^{\gamma}\right) \oplus H1\left(e\left(SK_{ID_i}, C\right)\right)$

$= Msg \oplus H1\left(e(H\left(ID_i\right)_i, sR)^{\gamma}\right) \oplus H1\left(e\left(SK_{ID_i}, \gamma . R\right)\right)$

$= Msg \oplus H1\left(e(s.H\left(ID_i\right)_i, R)^{\gamma}\right) \oplus H1\left(e\left(SK_{ID_i}, \gamma . R\right)\right)$

$= Msg \oplus H1\left(e(s.H\left(ID_i\right)_i, R)^{\gamma}\right) \oplus H1\left(e(s.H\left(ID_i\right)_i, R)^{\gamma}\right)$

$= Msg$

5.2 Comparison Scheme 2

Receivers use the same system parameters of Sender.

- Set up (Sender) Choose $P \in G1, Q \in G2,\ \gamma \longleftarrow Zp,$ $H:\{0,1\}^n \longrightarrow G1, H1:\{0,1\}^* \longrightarrow Zp$

$$Pub_s = \gamma Q$$

$$MSK_s = \gamma$$

- Encryption (Sender)

$$BK_i = SK_{ID_i} + m.H1\left(SK_{ID_i}\right).P$$

Where i=1, 2, 3…t

t=number of receivers

$$C = e(P, Q)^{\gamma . m}.Msg$$

- Set up (Receiver) Choose $R \in G1, V \in G2,\ s \in Zp$

$$Pub_c = sR$$

$$MSK_c = s$$

- Extraction (Receiver)

$$SK_{ID_i} = s.H(ID_i)$$

- Decryption (Receiver)

$$D = \frac{C}{K}$$

Calculate K first

$$K = e(Pub_s, BK_i - SK_{ID_i})^{\frac{1}{H1\left(SK_{ID_i}\right)}}$$

$$= e\left(\gamma Q, m.H1\left(SK_{ID_i}\right).P\right)^{\frac{1}{H1\left(SK_{ID_i}\right)}}$$

$$= e(P, Q)^{\gamma . m}$$

- Correctness

$$D = \frac{C}{K} = \frac{e(P,Q)^{\gamma . m}.Msg}{e(P,Q)^{\gamma . m}} = Msg$$

5.3 Comparisons

Public Key Length: The public key of our scheme is $Pub_c = \left(R, \frac{1}{s}V\right)$ for receiver and $Pub_s = (\frac{1}{\gamma}.P, Q)$ for sender. In all schemes, the public key length is constant. Therefore, complexity is O (1).

Private Key Length: For all schemes, the length of private key is O (1) as private keys are $SK_{ID_i} = s.H(ID_i)$ and $SK_{ID_i} = R^{1/s.H1(ID_i)}$.

Pairing Operations: In comparison scheme (1), sender has to do (n) pairings for (n) different users (data owners). In comparison with scheme (1), scheme (2) and our scheme need only one time pairing for message encryption.

Ciphertext Length: In both schemes (1) and (2), sender has to send (encrypted message for user 1, encrypted message for user 2, encrypted message for user n) and (encrypted message, broadcast key for user 1, broadcast key for user 2,.., broadcast key for user n) for (n) receivers respectively. Therefore, ciphertext length is proportional to the number of broadcast receivers. In our scheme, ciphertext length is constant.

Public Parameters Storage on Sender: In comparison scheme (1), sender has to store (n) different system parameters for (n) different users (data owners). However, in comparison scheme (2), all users (data owners) use the same system parameters of sender. In a similar fashion, our scheme also uses the same system parameters of sender. Therefore, storage for different parameters is not needed on the sender for scheme (2) and our scheme.

Broadcast Encryption Time: In comparison with broadcast encryption scheme [6], although key extraction time is lower, key encryption time is larger in scheme (1) and scheme (2). However, our scheme has nearly equal encryption time. In Figure 7, sender's broadcast encryption time of proposed scheme, comparison schemes and [6] is compared.

Sender Load: As sender's load, extract and encrypt time is integrated. Set up time is omitted as it is performed only one time before system starts up. Sender's load comparison is illustrated in Figure 8.

Table 1: Comparison Scheme (1) vs. Comparison Scheme (2)

	Comparison Scheme (1)	Comparison Scheme (2)
Public Key Length	O(1)	O(1)
Private Key Length	O(1)	O(1)
Pairing	n	1
Addition		N
Multiplication	n	n+1
Exponentiation	n	1
Decryption Cost	O(1)	O(1)
Key Extraction on Sender	N	N
Ciphertext Length	O(n)	O(n)
Public Parameters Storage on Sender	n	1
Broadcast Key Generation on Receiver	N	N

Table 2: Our Scheme vs. IBBE Scheme [6]

	IBBE [6]	Our Scheme
Public Key Length	O(1)	O(1)
Private Key Length	O(1)	O(1)
Encryption Cost	O(n)	O(n)
Decryption Cost	O(1)	O(1)
Key Extraction on Sender	Y	N
Ciphertext Length	O(1)	O(1)
Broadcast Key Generation on Receiver	N	Y

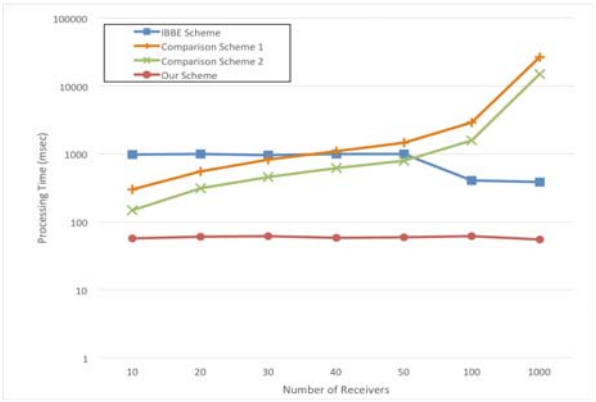

Figure 7: Encryption Time on Sender

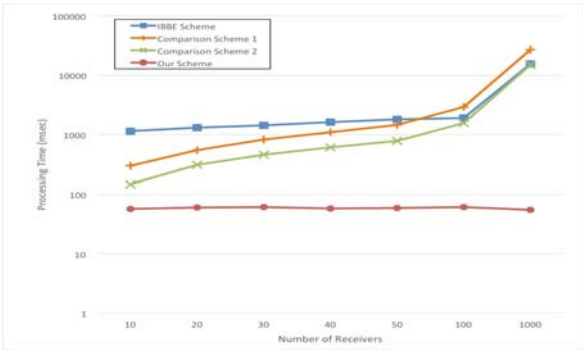

Figure 8: Sender's load for key extraction and encryption

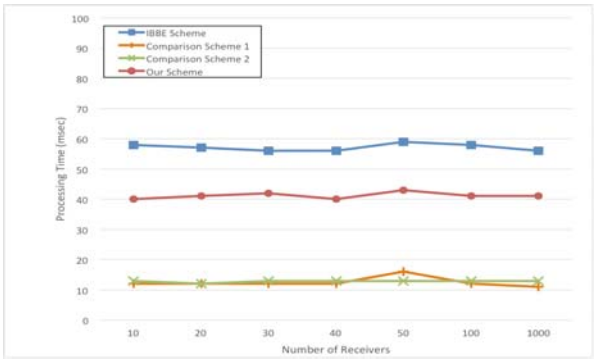

Figure 9: Decryption Time

6. Conclusion

We present three broadcast encryption schemes based on user-centric IBE scheme. Performance evaluation in terms of size of public key, private key, ciphertext and storage on sender has also been described. Among three broadcast schemes for user-centric IBE, our scheme achieves constant size of public key, private key, and ciphertext. Encryption time is nearly same to that of sender-centric IBBE scheme.

Acknowledgment

This research was partly supported by the collaborative research of National Institute of Information and Communications Technology (NICT) and Osaka University (Research on high functional network platform technology for largescale distributed computing).

Reference

[1] Wang, L. and Wu, C.-K.: "Efficient identity-based multicast scheme from bilinear pairing." *Communications, IEE Proceedings-*. Vol. 152. No. 6. IET, (2005).

[2] Wallner, D., Harder, E., and Agee, R.: Key management for multicast: Issues and architectures.No.RFC 2627, June (1999).

[3] Wong, CK., Gouda, M., and Lam, S.S.:"Secure group communications using key graphs." *Networking, IEEE/ACM Transactions on*8.1, pp. 16-30 (2000).

[4] Canetti, R., et al.: "Multicast security: A taxonomy and some efficient constructions." INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 2. IEEE, (1999).

[5] Delerablée, C.: "Identity-based broadcast encryption with constant size ciphertexts and private keys." *Advances in Cryptology–ASIACRYPT 2007*. Springer Berlin Heidelberg, pp. 200-215 (2007).

[6] Jiang, H., Xu, Q., and Shang, J.: "An efficient dynamic identity-based broadcast encryption scheme." *Data, Privacy and E-Commerce (ISDPE), 2010 Second International Symposium on*. IEEE, (2010).

[7] Baek, J., Safavi-Naini, R., and Susilo, W.: "Efficient multi-receiver identity-based encryption and its application to broadcast encryption." Public Key Cryptography-PKC 2005, Springer Berlin Heidelberg, pp. 380-397 (2005).

[8] Barbosa, M., and Farshim, P.: "Efficient identity-based key encapsulation to multiple parties." Cryptography and Coding. Springer Berlin Heidelberg, pp. 428-441 (2005).

[9] Mu, Y., Susilo, W., and Lin,Y.: "Identity-based broadcasting.*"Progress in Cryptology-INDOCRYPT 2003*. Springer Berlin Heidelberg, pp. 177-190 (2003).

[10] Delerablée, C., Paillier, P., and Pointcheval, D.: "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys." *Pairing-Based Cryptography–Pairing 2007*. Springer Berlin Heidelberg, pp. 39-59 (2007).

[11] Boneh, D., Gentry, C., and Waters, B.: "Collusion resistant broadcast encryption with short ciphertexts and private keys." *Advances in Cryptology–CRYPTO 2005*. Springer Berlin Heidelberg, (2005).

[12] Sakai, R., and Furukawa, J.: "Identity-Based Broadcast Encryption."*IACR Cryptology ePrint Archive* 2007, (2007).

[13] Hu, L., Liu, Z., and Cheng, X.: "Efficient Identity-based broadcast encryption without random oracles." Journal of Computers 5.3, pp. 331-336 (2010).

[14] https://en.wikipedia.org/wiki/Pairing-based_cryptography

[15] Shamir, A.: Identity-based cryptosystems and signature schemes In CRYPTO 84, pp. 47–53 (1984).

[16] Boneh, D., and Franklin, M.: "Identity-based encryption from the

Weil pairing." *Advances in Cryptology—CRYPTO 2001*. Springer Berlin Heidelberg, (2001).

[17] Melige, A., Abdo, A., and Alazah, A.: “P2P Social Network with Dynamic Identity-based Broadcast Encryption using Rolls.” International Journal of Computer Applications, pp. 14-17 (2014).

[18] Kaaniche, N., Boudguiga, A., and Laurent, M.: “ID Based Cryptography for Cloud Data Storage.” Proceedings of the 2013 IEEE Sixth International Conference on Cloud Computing, IEEE Computer Society, (2013).