Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 329198, 7 pages
http://dx.doi.org/10.1155/2014/329198

Research Article

Time-and-ID-Based Proxy Reencryption Scheme

Kambombo Mtonga,[1] Anand Paul,[2] and Seungmin Rho[3]

[1] *Department of IT Convergence and Engineering, Kyungil University, Daegu 712-701, Republic of Korea*
[2] *School of Computer Science and Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea*
[3] *Department of Multimedia, Sungkyul University, Anyang-si 430-742, Republic of Korea*

Correspondence should be addressed to Seungmin Rho; smrho@sungkyul.ac.kr

Received 28 December 2013; Accepted 4 February 2014; Published 22 May 2014

Academic Editor: Jongsung Kim

Time- and ID-based proxy reencryption scheme is proposed in this paper in which a type-based proxy reencryption enables the delegator to implement fine-grained policies with one key pair without any additional trust on the proxy. However, in some applications, the time within which the data was sampled or collected is very critical. In such applications, for example, healthcare and criminal investigations, the delegatee may be interested in only some of the messages with some types sampled within some time bound instead of the entire subset. Hence, in order to carter for such situations, in this paper, we propose a time-and-identity-based proxy reencryption scheme that takes into account the time within which the data was collected as a factor to consider when categorizing data in addition to its type. Our scheme is based on Boneh and Boyen identity-based scheme (BB-IBE) and Matsuo's proxy reencryption scheme for identity-based encryption (IBE to IBE). We prove that our scheme is semantically secure in the standard model.

1. Introduction

A proxy reencryption (PRE) scheme involves three parties: delegator (Alice), delegatee (Bob), and a proxy (semitrusted third party). Alice assigns a key to a proxy to reencrypt all her messages encrypted with her public key such that the reencrypted ciphertexts can be decrypted with Bob's private key. Due to this delegation of decrypting capability, various applications of PRE have been suggested, for example, email forwarding, digital rights management (DRM), law enforcement, and secure network file storage [1–4]. Charlie provides multiple-hop or multiuse proxy to the systems while PRE schemes could be defined based on the direction of operation, number of hops (possible reencryption), and their structure. *Unidirectional* PRE implies that the proxy can reencrypt a message from Alice to Bob but cannot reencrypt a message from Bob to Alice using the same key, while *bidirectional* PRE applies from sender to recipient and vice versa. PRE schemes capable of reencrypting a message from Alice to Bob and then from Bob to Charlie are said to be a multihop or multi-use proxy [5, 6]. On the other hand, single-hop schemes use a specific key to reencrypt between only two entities. It is important that the PRE scheme should at least satisfy the following requirements: (1) a proxy alone cannot obtain the underlying plaintext and (2) delegatee cannot obtain the underlying plaintext without the proxy's cooperation.

Based on a simple modification of the ElGamal encryption scheme, Blaze et al. [7] in 1998 proposed the first PRE scheme where the proxy is kept from knowing plaintexts and secret keys [8]. Ateniese et al. [1] proposed a number of unidirectional PRE schemes and discussed their several potential applications such as distributed secure file systems. Later, many unidirectional PRE schemes with different properties have been proposed [9–11]. In recent past, the concept of identity-based proxy reencryption (IB-PRE) has gained popularity among researchers [12, 13]. It (IBE) was first introduced by Shamir [14]. The main idea of ID-based cryptosystems is that the identity information of each user (such as E-mail addresses, security number, or IP addresses) works as his/her public key. In other words, the user's public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA) as is the case in certificate-based cryptosystems. ID-based public key setting serves as a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. After Boneh and Franklin [15] proposed a practical IBE scheme, Green and Ateniese later [16] proposed the first IB-PRE scheme. IB-PRE is IBE which permits delegation of decryption capability. They also discussed its several interesting applications such as bridging IBE and public key encryption (PKE). Since then, several IB-PRE schemes have been proposed [17, 18]. In IB-PRE, a user who has a secret key corresponding to his/her public identity can decrypt a ciphertext encrypted with his/her identity as in IBE. In 2007, Matsuo proposed the concept of four types of PRE schemes: certificate-based PKE (CBE) to CBE, IBE to CBE, CBE to IBE, and IBE to IBE [19]. Matsuo's schemes are based on ElGamal-type CBE scheme and BB-IBE [20]. Now CBE to IBE and IBE to IBE PRE schemes are being standardized by IEEEP1363.3 working group [21].

In 2008, Tang [22] first introduced the concept of type-based PRE (TB-PRE). He proposed two schemes; one scheme achieved ciphertext privacy and was proved chosen plaintext attack (IND-PR-CPA) secure under the eXternalDiffie-Hellman (XDH) and co-BDH assumptions, while the other scheme achieved chosen ciphertext attack (IND-PR-CCA) security under the knowledge of exponent (KE) and the bilinear Diffie-Hellman (BDH) assumptions. In a TB-PRE scheme, the delegator categorizes his/her messages (ciphertexts) into different subsets and is capable of delegating the decryption right of each subset to a specific delegatee. The ciphertexts for the delegator are generated based on the delegator's public key and the message type which is used to identify the message subset. TB-PRE as a variant of PRE could be considered as a subset of conditional proxy reencryption (C-PRE). In C-PRE schemes, ciphertexts are generated with respect to a certain condition and the proxy can translate a ciphertext only if the associated condition is satisfied [23, 24]. Ibraimi et al. [25] proposed the first type-and-identity-based proxy reencryption (TIB-PRE) scheme based on the Boneh-Franklin IBE scheme. Their scheme was proved semantically secure against an adaptive chosen plaintext attack for the delegator (IND-ID-DR-CPA). They further showed how their scheme could be used by a patient to enforce his/her personal health record (PHR) disclosure policies. A TIB-PRE scheme is basically a TB-PRE scheme that encompasses IBE and PRE.

1.1. Motivation and Contribution. As pointed out in [22, 25], the existing PRE schemes have a limitation in that the proxy could reencrypt all ciphertexts encrypted under delegator's public key and pass them to the delegatee. In order to implement fine-grained access control policies, the delegator (1) can choose a different key pair for each possible subset of his/her messages and choose a proxy to delegate his decryption right or (2) can choose to trust the proxy to enforce his policies by reencrypting the predefined subset of his ciphertexts to the specific delegatee. However, both of these approaches are infeasible in practice because they are too involving for the delegator and also demand strong trust on the proxy. On the other hand, in a type-based proxy reencryption scheme, the delegator can categorize his messages (ciphertexts) into different subsets and is capable of delegating the decryption right of each subset to a specific delegatee. Hence, type-based proxy reencryption enables the delegator to implement fine-grained policies with one key pair and without any additional trust on the proxy.

Despite this advantage, however, in some applications, instead of delegating all the messages under a type-based subset, the delegator may be required to delegate just some of the messages within the subset. This may be because the delegate could be interested in specific messages collected or sampled within a specified period of time. For example, (1) in healthcare, a physician maybe interested only in a patient's recent (e.g., last five months) prescription history to check if his/her recent drug interactions could conflict with the proposed course of treatment. (2) In criminal investigations, an investigator may only be interested in video footage from closed circuit television recordings (CCTV) of the crime scene that were taken within the time bound of the occurrence of the crime. In view of such cases, we argue that incorporating an element of time period (e.g., hours, days, etc.) in TBE would give the delegator more flexibility to provide the proxy with more fine-grained reencryption capabilities. Hence, in this paper we propose a time-and-identity-based proxy reencryption scheme (t_m-IB-PRE) to solve aforementioned shortfalls in PRE schemes while at the same time adopting the advantages of TB-PRE and IBE schemes. Our scheme is based on BB-IBE and Matsuo's IBE to IBE PRE schemes. Unlike the existing TB-PRE schemes, the ciphertexts for the delegator in our scheme are generated based on the delegator's public key and some specified time periods. We find this assumption plausible because it is common practice to attach date and even time to data upon its collection. Note that our scheme can be considered as a special case of TBE. As such we assume that the delegator will first categorize his/her messages into subsets according to type and then, as may be requested by the delegatee, the delegator can further recategorizes the messages into refined subsets depending on specified time period. The reencryption key in our scheme is independent of the delegatee's private key. As a result, our scheme can achieve master secret security.

2. Preliminaries

In this section, we first review the basic concept of the bilinear maps and related assumptions. Then, a brief discussion of IBE and TIB-PRE together with their respective security models will follow [26].

Definition 1. Let G and G_1 be two cyclic multiplicative groups with prime order p. Let g be a generator of G and let $\hat{e}$: $G \times G \to G_1$ be a bilinear map with the following properties.

(i) *Bilinearity*: for all $u, v \in G$ and for all $a, b \in Z$, we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$.

(ii) *Nondegeneracy*: the map does not send all pairs in $G \times G$ to the identity in G_1. Observe that since G and G_1 are groups of prime order this implies that if g is a generator of G, then $\hat{e}(g, g)$ is a generator of G_1. G

is said to be a bilinear group if the group operation in G and the bilinear map $\hat{e}: G \times G \rightarrow G_1$ are both efficiently computable.

We assume that there is an efficient algorithm *Gen* for generating bilinear groups. The algorithm *Gen* takes a security parameter k as input and outputs a tuple $(p, G, G_1, g$, and $\hat{e})$.

Definition 2. The decisional bilinear Diffie-Hellman (dBDH) problem in groups (G, G_1) is as follows. Given $(g, g^a, g^b, g^c, X) \in G \times G_1$ with unknown $a, b, c \in_R Z_p^*$, decide whether $X = \hat{e}(g, g)^{abc}$. The advantage of an algorithm $\mathscr{A}$ in solving the dBDH problem is defined as follows:

$$\begin{aligned}\mathrm{Adv}_G^{\mathrm{dBDH}}(\mathscr{A}) = \Big| \Pr\left[\mathscr{A}\left(g, g^a, g^b, g^c, \hat{e}(g,g)^{abc}\right) = 0\right] \\ - \Pr\left[\mathscr{A}\left(g, g^a, g^b, g^c, X\right) = 0\right]\Big|,\end{aligned} \tag{1}$$

where the probability is over the random choice of generator $g \in_R G$, the randomly chosen integers $a, b, c \in_R Z_p^*$, the random choice of $X \in_R G_1$, and the random bits used by $\mathscr{A}$. We say that the $(k, t, \varepsilon\text{-})$ dBDH assumption holds in G if no t-time algorithm has advantage at least ε in solving the dBDH problem in G under a security parameter k.

2.1. Definition and Security Notion for IBE

Definition 3. An IBE scheme consists of four algorithms: $Setup_{IBE}$, $KeyGen_{IBE}$, $Encrypt_{IBE}$, and $Decrypt_{IBE}$ [27].

$Setup_{IBE}(1^k)$. This algorithm takes a security parameter k as input and outputs parameters *params* which are distributed to users and the master key *mk* which is kept private.

$KeyGen_{IBE}$(*params, mk, id*). This algorithm takes parameters *params*, the master key *mk,* and an identifier *id* as input and it outputs a private key d_{id} associated with *id*.

$Encrypt_{IBE}$(*params, M, id*). This algorithm takes parameters *params*, a message *M,* and an identifier *id* as input and outputs a ciphertext C_{id} encrypted under *id*.

$Decrypt_{IBE}(C_{id}, d_{id})$. This algorithm takes a ciphertext C_{id} associated with an identifier *id* as input and outputs a message M or $\perp$ as an error message.

Definition 4. The selective identity chosen plaintext (IND-sID-CPA) security for an IBE scheme is defined as a game between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$, where the challenger simulates the protocol execution and answers queries from the adversary.

Initialization. The adversary outputs an identifier id^* where it wishes to be challenged.

$Setup_{IBE}$. The challenger runs the setup algorithm and returns parameters *params* to the adversary while keeping the master key *mk* to itself.

Phase 1. The adversary adaptively issues $q_1 \cdots q_m$ private key queries for $id_i \neq id^*$. The challenger runs the algorithm $KeyGen_{IBE}$ and outputs the private keys d_{id_i} corresponding to id_i. The challenger sends d_{id_i} to the adversary.

Once adversary decides that phase 1 is over, it selects two equal length plaintexts $M_0, M_1 \in M$ on which it wishes to be challenged.

Challenge. Given $(M_0,\ M_1,\ id^*)$, the challenger picks a random bit $b \in_R \{0, 1\}$ and sends the challenge ciphertext $C^* = Encrypt_{IBE}(params, M_b, id^*)$ to the adversary.

Phase 2. The adversary continues to issue $q_{m+1} \cdots q_n$ queries as in phase 1 but with restriction that he/she cannot issue private key queries for $id_i = id^*$. The challenger responds as in phase 1.

Guess. Finally, the adversary issues a guess $b' \in_R \{0, 1\}$. The adversary wins the game if $b' = b$.

An IBE scheme is IND-sID-CPA secure if $|\Pr[b' = b] - 1/2|$ is negligible.

Definition 5. We define the advantage of adversaries in an IND-sID-CPA games as

$$\mathrm{Adv}_A^{\mathrm{game}} = \left(\Pr\left[b' = b\right] - \frac{1}{2}\right). \tag{2}$$

An IBE system is said to be $(k, t, q, \varepsilon\text{-})$ IND-sID-CPA secure if for any t-time IND-sID-CPA adversary $\mathscr{A}$ that makes at most q chosen secret key queries under a security parameter k we have $\mathrm{Adv}_A^{\mathrm{game}} < \varepsilon$. As shorthand, we say that an IBE system is $(k, t, q, \varepsilon\text{-})$ IND-sID-CPA secure.

2.2. Definition and Security Notion for TIBE and TIB-PRE Scheme

Definition 6. We base our definitions on [22, 25]. A TIBE scheme consists of four algorithms: $Setup_{TIBE}$, $KeyGen_{TIBE}$, $Encrypt_{TIBE}$, and $Decrypt_{TIBE}$. Both $Setup_{TIBE}$ and $KeyGen_{TIBE}$ are run under IBE. Below, we define $Encrypt_{TIBE}$ and $Decrypt_{TIBE}$. Note that we adopt the notation T to stand for message type.

$Encrypt_{TIBE}$(*params, M, id, T*). This algorithm takes parameters *params*, a message M, an identifier *id*, and a message type T as input and it outputs a ciphertext C_{id} encrypted under *id*. Both C_{id} and T are sent to the receiver.

$Decrypt_{TIBE}(C_{id}, d_{id}, T)$. This algorithm takes the ciphertext C_{id}, the private key d_{id}, and a message type T as input. The algorithm outputs a message M of type T.

Definition 7. A TIB-PRE scheme is a PRE that combines the concepts of both IBE and type-based encryption. The scheme consists of six algorithms: $Setup_{TIB\text{-}PRE}$, $Key\ Gen_{TIB\text{-}PRE}$, $Pextract_{TIB\text{-}PRE}$, $Encrypt_{TIB\text{-}PRE}$, $Preenc_{TIB\text{-}PRE}$, and $Decrypt_{TIB\text{-}PRE}$. $Setup_{TIB\text{-}PRE}$, $KeyGen_{TIB\text{-}PRE}$, *Encrypt*$_{TIB\text{-}PRE}$, and *Decrypt*$_{TIB\text{-}PRE}$ are defined as above. Below we define *Pextract*$_{TIB\text{-}PRE}$ and *Preenc*$_{TIB\text{-}PRE}$.

Pextract$_{TIB\text{-}PRE}(d_{id} id, id', T)$. This algorithm is run by the delegator. It takes a delegator's private key d_{id}, the delegator's identifier id, the delegatee's identifier id', and a message type T as input. The algorithm outputs $rk_{id \rightarrow id'}$ as the reencryption key.

Preenc$_{TIB\text{-}PRE}(C_{id}, rk_{id \rightarrow id'}, T)$. This algorithm is run by the proxy. It takes the ciphertext C_{id} associated with delegator's identifier, the reencryption key $rk_{id \rightarrow id'}$, and a message type T as input. The algorithm outputs a new ciphertext C' for delegatee.

Definition 8. We model selective identity chosen plaintext security for a TIB-PRE scheme as a game between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$, where the challenger simulates the protocol execution and answers queries from the adversary.

Initialization. The adversary outputs an identity id^* and T^* where it wishes to be challenged.

Setup$_{TIB\text{-}PRE}$. The challenger runs the setup algorithm and returns parameters *params* to the adversary while keeping the master key *mk* to itself.

Phase 1. Taking parameters *params* as input, the adversary adaptively issues the following queries.

PrivateKeyquery$_{TIB\text{-}PRE}$. The adversary queries with any identifier $id_i \neq id^*$. The challenger outputs private keys d_{id_i} corresponding to id_i. The challenger sends d_{id_i} to adversary.

Pextract$_{TIB\text{-}PRE}$. The adversary queries with (id_i, id', T). If id' has been queried to a private key query, then the challenger halts. Otherwise, the challenger outputs a reencryption key $rk_{id \rightarrow id'}$ for type T and sends it to the adversary.

Preenc$_{TIB\text{-}PRE}$. The adversary queries the challenger with (M, id, id', T). The challenger first computes C_{id} = *Encrypt*$_{TIB\text{-}PRE}(M, id, T)$ and returns C' = *Preenc*$_{TIB\text{-}PRE}(C_{id}, rk_{id \rightarrow id'}, T)$ to the adversary which is obtained by applying the delegation key $rk_{id \rightarrow id'}$ to C_{id}.

Once adversary decides that phase 1 is over, it selects two equal length plaintexts $M_0, M_1 \in M$ on which it wishes to be challenged.

Challenge. The challenger picks a random bit $b \in_R \{0, 1\}$ and sets the challenge ciphertext to C^* = *Encrypt*$_{TIB\text{-}PRE}$(*params*, M_b, id^*, T^*). It sends C^* as the challenge to the adversary.

Phase 2. The adversary continues to issue queries as in phase 1 but with restrictions that

(i) he/she cannot issue private key queries for $id_i = id^*$;

(ii) if there is a *Preenc*$_{TIB\text{-}PRE}$ query with (M, id, id^*, T), then (id, id^*, T) has not been queried to *Pextract*$_{TIB\text{-}PRE}$.

The challenger responds as in phase 1.

Guess. Finally, the adversary outputs a guess $b' \in_R \{0, 1\}$. The adversary wins if $b = b'$.

At the end of the game, the adversary's advantage is defined to be $\mathrm{Adv}_A^{\mathrm{game}} = (\Pr[b' = b] - 1/2)$.

3. Our Construction

In this section, we propose our time-and-identity-based proxy reencryption scheme (t_m-IB-PRE) based on BB-IBE and Matsuo ID-PRE scheme. We adopt the basic principles of TIB-PRE. First we describe our t_m-IBE scheme followed by a discussion of the delegation process. In our scheme, we assume one level delegation, meaning that the delegatees will not further delegate their decryption rights to other users. We adopt t_m to denote some specified period of time (date, month, or year). Our scheme consists of six algorithms, namely, *Setup*, *KeyGen*, *Pextract*, *Encrypt*, *Preenc,* and *Decryp*.

Setup(1^k). This algorithm is run by the PKG and works as follows: it takes the security parameter k and selects a random generator $g \in G$ and random element $g_2 \in_R G$. Pick a random $\alpha \in_R Z_p^*$ and set $g_1 = g^{\alpha}$, $mk = g_2^{\alpha}$, and $params = (g, g_1, g_2)$. Here, $mk = \alpha$ is the master secret key and *params* are public parameters.

KeyGen(*params, mk, id*). Here, the PKG takes parameters *params*, master key $mk = \alpha$, and an identifier id as input. The PKG picks a random value $x \in_R Z_p^*$ and outputs a private key d_{id} corresponding to id, where

$$d_{id} = (y_0, y_1) = \left(g_2^{\alpha}\left(g_1^{id}\right)^{x}, g^{x}\right). \tag{3}$$

Encrypt(*params, M, id,* t_m). To encrypt a message M bounded by time t_m, the message sender picks $r \in_R Z_p^*$ at random, computes $Y = \hat{e}(g_1, g_2)$, and outputs ciphertext C_{id}, where

$$C_{id} = (c_1, c_2, c_3, c_4) = \left(g^{r}, \left(g_1^{id}\right)^{rt_m}, MY^{rt_m}, t_m\right). \tag{4}$$

Note that $Y = \hat{e}(g_1, g_2)$ can be precomputed once and for all so that encryption does not require any pairing computations.

Decrypt(C_{id}, d_{id}, t_m). On inputting a ciphertext $C_{id} = (c_1, c_2, c_3, c_4)$, a private key $d_{id} = (y_0, y_1)$, and t_m, the algorithm outputs M as follows:

$$\begin{aligned} M &= \frac{c_3 \hat{e}\left(y_1, c_2\right)}{\hat{e}\left(y_0, \left(c_1\right)^{c_4}\right)} = \frac{M\hat{e}(g_1, g_2)^{rt_m} \cdot \hat{e}\left(g^{x}, g_1^{idrt_m}\right)}{\hat{e}\left(g_2^{\alpha}(g_1^{id})^{x}, g^{rt_m}\right)} \\ &= \frac{M\hat{e}(g, g_2)^{\alpha rt_m} \cdot \hat{e}(g, g_1)^{idrxt_m}}{\hat{e}(g_2, g)^{\alpha rt_m} \cdot \hat{e}(g_1, g)^{idrxt_m}} = M. \end{aligned} \tag{5}$$

3.1. Delegation Process. To delegate his decryption right for some message subsets, the delegator makes use of the following algorithms.

Pextract(d_{id}, id, id', t_m). This algorithm is run by the delegator. It takes private key of delegator $d_{id} = (y_0, y_1)$, an identifier of delegator id and that of delegate id', and sometime period t_m as input. The algorithm outputs a reencryption key $rk_{id \to id'} = (s_0, s_1, s_2) = (y_0 v, y_1, B)$, where $v = (id \| l \| id' \parallel t_m)$ and $B = Encrypt(params, v, id', t_m)$, $l \in_R Z_p^*$.

Preenc$(C_{id}, rk_{id \to id'})$. This algorithm is run by the proxy. It takes a reencryption key $rk_{id \to id'} = (s_0, s_1, s_2)$ and a ciphertext $C_{id} = (c_1, c_2, c_3, c_4)$, where $t_m = c_4$. The algorithm outputs a new ciphertext $C' = (w_1, w_2, w_3, w_4)$, where

$$w_1 = c_3 \frac{\hat{e}(s_1, c_2)}{\hat{e}\left(s_0, (c_1)^{c_4}\right)}, \qquad w_2 = c_1, \qquad w_3 = c_4, \qquad w_4 = s_2. \tag{6}$$

Once delegatee receives the reencrypted ciphertext, he/she can obtain the plaintext by computing

$$\begin{aligned}
M &= \frac{w_1}{\hat{e}\left((w_2)^{w_3}, Decrypt\,(w_4, d_{id'})\right)^{-1}} \\
&= \frac{c_3\left(\hat{e}(s_1, c_2) / \hat{e}\left(y_0 v, (c_1)^{c_4}\right)\right)}{\hat{e}\left((c_1)^{c_4}, Decrypt\,(s_2, d_{id'})\right)^{-1}} \\
&= \frac{c_3\left(\hat{e}(s_1, c_2) / \hat{e}\left(y_0, (c_1)^{c_4}\right) \cdot \hat{e}\left(v, (c_1)^{c_4}\right)\right)}{\hat{e}\left((c_1)^{c_4}, Decrypt\,(s_2, d_{id'})\right)^{-1}} \\
&= \left(M\hat{e}(g_1, g_2)^{rt_m} \frac{\hat{e}\left(g^x, g_1^{idrt_m}\right)}{\hat{e}\left(g_2^{\alpha}\left(g_1^{idx}\right), g^{rt_m}\right) \cdot \hat{e}\left(v, g^{rt_m}\right)}\right) \\
&\quad \times \left(\hat{e}\left(g^{rt_m}, \mathbf{v}\right)^{-1}\right)^{-1} \\
&= \left(\frac{M\hat{e}(g, g_2)^{\alpha rt_m} \cdot \hat{e}(g, g_1)^{idxrt_m}}{\hat{e}(g_2, g)^{\alpha rt_m} \cdot \hat{e}(g_1, g)^{idxrt_m} \cdot \hat{e}\left(v, g^{rt_m}\right)}\right) \\
&\quad \times \left(\hat{e}\left(g^{rt_m}, \mathbf{v}\right)^{-1}\right)^{-1} \\
&= \frac{M / \hat{e}\left(v, g^{rt_m}\right)}{\hat{e}\left(v, g^{rt_m}\right)^{-1}} = M.
\end{aligned} \tag{7}$$

3.2. Security Analysis

Theorem 9. *Suppose that the* $(k, t, \varepsilon$-) *dBDH assumption holds in G. Then, the proposed* t_m*-IB-PRE scheme is* (k, t', q, ε') *selective identity (IND-sID-CPA) secure for any* q, k, $\varepsilon' \leq \varepsilon$ *and* $t' = t - \Theta(\tau q)$, *where* τ *is maximum time for an exponentiation in G.*

Proof. Let $\mathscr{A}$ be an adversary against the proposed t_m-IB-PRE scheme in the IND-sID-CPA sense. We construct an adversary $\mathscr{B}$ which solves the dBDH problem in G by utilizing $\mathscr{A}$. Algorithm $\mathscr{B}$ is given $(g, J_1, J_2, J_3, U) = (g, g^a, g^b, g^c, U)$ as input, where $U = \hat{e}(g, g)^{abc}$ or $U = X \in_R G_1$ and $a, b, c \in_R Z_p^*$. Algorithm $\mathscr{B}$ works by interacting with $\mathscr{A}$ in a selective identity game as follows.

Initialization. The selective identity game begins with $\mathscr{A}$ outputting a target identity id^* and some fixed t_m^*.

Setup. To generate system parameters, algorithm $\mathscr{B}$

(i) picks $\beta \in_R Z_p^*$;

(ii) sets $g_1 = J_1$ and $g_2 = J_2$ and gives parameters *params* $= (g, g_1, g_2)$ to $\mathscr{A}$. The corresponding master key unknown to $\mathscr{B}$ is $g_2^a = g^{ab}$.

Phase 1. Taking parameters *params* as input, the adversary adaptively issues the following queries.

Private Keyqueries. $\mathscr{A}$ queries with any identifier $id_i \neq id^*$. $\mathscr{B}$ outputs private keys d_{id_i} corresponding to id_i and sends it to $\mathscr{A}$. Here,

$$\begin{aligned}
d_{id_i} &= (y_0, y_1) \\
&= \left(g_2^{-\beta/(id_i - id^*)}\left(g_1^{id_i - id^*} g^{\beta}\right)^{r_i}\left(g_1^{-id^*} g^{\beta}\right)^{-r_i}, \right. \\
&\qquad \left. g_2^{-1/(id_i - id^*)} g^{r_i}\right), \quad \text{where } r_i \in_R Z_p^*.
\end{aligned} \tag{8}$$

Let $x = r_i - (b/(id - id^*))$; then d_{id_i} is valid private key for id_i. This is because

$$\begin{aligned}
d_{id_i} &= (y_0, y_1) \\
&= \left(g_2^{-\beta/(id_i - id^*)}\left(g_1^{id_i - id^*} g^{\beta}\right)^{r_i}\left(g_1^{-id^*} g^{\beta}\right)^{-r_i}, \right. \\
&\qquad \left. g_2^{-1/(id_i - id^*)} g^{r_i}\right), \quad \text{where } r_i \in_R Z_p^* \\
&= \left(\frac{g_2^{-\beta/(id_i - id^*)}\left(g_1^{id_i - id^*} g^{\beta}\right)^{r_i}\left(g_1^{-id^*} g^{\beta}\right)^{-r_i}}{\left(g_1^{id_i}\right)^{b/(id_i - id^*)}}, \right. \\
&\qquad \left. g^{r_i - (b/(id_i - id^*))}\right) \\
&= \left(\frac{g_2^{a}\left(g_1^{id}\right)^{r_i}\left(g_1^{-id^*} g^{\beta}\right)^{r_i}\left(g_1^{-id^*} g^{\beta}\right)^{-r_i}}{\left(g_1^{id_i}\right)^{b/(id_i - id^*)}}, \right. \\
&\qquad \left. g^{r_i - (b/(id_i - id^*))}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{g_2^a \left(g_1^{id}\right)^{r_i}}{\left(g_1^{id_i}\right)^{b/(id_i - id^*)}}, g^{r_i - (b/(id_i - id^*))} \right) \\
&= \left(g_2^a \left(g_1^{id}\right)^{r_i - (b/(id_i - id^*))}, g^{r_i - (b/(id_i - id^*))} \right) \\
&= \left(g_2^a \left(g_1^{id}\right)^{x}, g^{x} \right).
\end{aligned}
\tag{9}
$$

Pextract$_{TIB\text{-}PRE}$. $\mathscr{A}$ queries with (id, id', t_m). If $id \neq id^*$ (in this case, id' can be any identity), the simulator $\mathscr{B}$ first simulates $KeyGen(params, mk, id)$ as above and gets d_{id}. Then, it runs $Pextract(params, d_{id}, id', t_m)$ and returns the resulting reencryption key $rk_{id \rightarrow id'}$ to the adversary. Otherwise, if $id = id^*$, $\mathscr{B}$ rejects the query.

Preenc. $\mathscr{A}$ queries the challenger with (M, id, id', t'_m). $\mathscr{B}$ only faithfully responds to this query if $id \neq id^*$ and $t'_m \neq t_m{}^*$. Otherwise, $\mathscr{B}$ halts.

Once adversary decides that phase 1 is over, it selects two equal length plaintexts $M_0, M_1 \in M$ on which it wishes to be challenged.

Challenge. The challenger picks a random bit $b \in_R \{0, 1\}$ and sets the challenge ciphertext to $C^* = (c_1^*, c_2^*, c_3^*, c_4^*) = (\text{Ꝁ}_1, (\text{Ꝁ}_2{}^{\beta})^{c_4^*}, M_b U^{c_4^*}, c_4^*)$, where $c_4^* = t_m^*$. $\mathscr{B}$ returns C^* to the adversary. Note that if $U = \widehat{e}(g, g)^{abc} = \widehat{e}(g_1, g_2)^c$, then C^* is valid encryption of M_b. Otherwise, if U is uniform and independent in G_1, then M_b is also independent of b in the adversary's view.

Phase 2. The adversary issue further queries $\mathscr{A}$ and $\mathscr{B}$ responds as in phase 1.

Guess. Finally, $\mathscr{A}$ outputs a guess $b' \in_R \{0, 1\}$. Algorithm $\mathscr{B}$ concludes its own game by outputting a guess as follows. If $b = b'$, then $\mathscr{B}$ outputs 1 meaning $U = \widehat{e}(g, g)^{abc}$. Otherwise, it outputs 0 meaning $U \neq \widehat{e}(g, g)^{abc}$.

$\mathscr{B}$ can perfectly simulate the reencryption key for id since it looks random and independent of any other values if $\mathscr{A}$ does not obtain the corresponding private key for id. When $U = \widehat{e}(g, g)^{abc}$, then $\mathscr{A}$'s advantage is the same as $\mathscr{B}$'s advantage for solving dBDH problem. □

4. Conclusion

In this paper, a time-and-identity based proxy reencryption scheme based on BB-IBE and Matsuo's PRE scheme has been proposed. Our scheme incorporates concept of time and gives the delegator the flexibility to categorize his/her message into subsets based on some defined time period. We have proven our scheme to be selective identity, chosen plaintext attack (IND-sID-CPA) secure in the standard model based on the decisional BDH assumption in the bilinear groups. Using only one key pair, the delegator in the scheme can provide the proxy with differentiated reencryption capabilities. This work can also be extended and included in various other fields [28–32] including m2m, IoT, and big data.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (no. NRF-13S1A5B6044042).

References

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[2] K. H. Choi, K. S. Jang, and H. J. Shin, "Smart home environment for the protection of multimedia digital contents," *The Journal of IWIT*, vol. 11, no. 2, pp. 189–196, 2011.

[3] C. Chu and W. Tzeng, "Identity-based proxy re-encryption without random oracles," in *Information Security*, vol. 4779 of *Lecture Notes in Computer Science*, pp. 189–202, 2007.

[4] E. B. Kim, K. I. Kim, T. H. Kim, and S. H. Cho, "A study of partial preview control method of ePUB-based eBook DRM," *The Journal of IWIT*, vol. 12, no. 1, pp. 249–256, 2012.

[5] G. Ateniese and S. Hohenberger, "Proxy re-signatures: new definitions, algorithms, and applications," in *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS '05)*, pp. 310–319, November 2005.

[6] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *Proceedings of the 15th ACM conference on Computer and Communications Security (CCS '08)*, pp. 511–520, October 2008.

[7] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in cryptology—EUROCRYPT*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 127–144, 1998.

[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science*, pp. 10–18, 1985.

[9] J. Shao, Z. Cao, and P. Liu, "SCCR: a generic approach to simultaneously achieve CCA security and collusion-resistance in proxy re-encryption," *Security and Communication Networks*, vol. 4, no. 2, pp. 122–135, 2011.

[10] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)*, pp. 322–332, March 2009.

[11] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *Public Key Cryptography—PKC*, vol. 4939 of *Lecture Notes in Computer Science*, pp. 360–379, 2008.

[12] L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New identity-based proxy re-encryption schemes to prevent collusion

attacks," in *Pairing-Based Cryptography-Pairing*, vol. 6487 of *Lecture Notes in Computer Science*, pp. 327–346, 2010.

[13] Z.-M. Wan, J. Weng, X.-J. Lai, S.-L. Liu, and J.-G. Li, "On the relation between identity-based proxy re-encryption and mediated identity-based encryption," *Journal of Information Science and Engineering*, vol. 27, no. 1, pp. 243–259, 2011.

[14] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology—Crypto*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, 1985.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, 2001.

[16] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proceedings of the 5th international conference on Applied Cryptography and Network Security (ACNS '07)*, J. Katz and M. Yung, Eds., vol. 4521, pp. 288–306, 2007.

[17] C. Chu and W. Tzeng, "Identity-based proxy re-encryption without random oracles," in *Information Security*, vol. 4779, pp. 189–202, 2007.

[18] C. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional proxy broadcast re-encryption," in *Information Security and Privacy*, vol. 5594 of *Lecture Notes in Computer Science*, pp. 327–342, 2009.

[19] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in *Pairing-Based Cryptography—Pairing 2007*, vol. 4575 of *Lecture Notes in Computer Science*, pp. 246–267, 2007.

[20] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 223–238, 2004.

[21] L. Martin, *P1363.3(TM)/D1, Draft Standard For Identity-Based Public Cryptography Using Pairings*, 2008.

[22] Q. Tang, "Type-based proxy re-encryption and its construction," in *Progress in Cryptology—INDOCRYPT*, vol. 5365 of *Lecture Notes in Computer Science*, pp. 130–144, 2008.

[23] J. Weng, Y. Yang, Q. Tang, R. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosen ciphertext security," in *Information Security*, P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, Eds., vol. 5735 of *Lecture Notes in Computer Science*, pp. 151–166, 2009.

[24] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09)*, pp. 322–332, March 2009.

[25] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identity-based proxy re-encryption scheme and its application in healthcare," *Secure Data Management*, vol. 5159, pp. 185–198, 2008.

[26] X. A. Wang, X. Yang, and Y. Han, "New identity based encryption and its proxy re-encryption," *Biomedical Engineering and Computer Science*, vol. 1, no. 4, pp. 23–25, 2010.

[27] S. Luo, Q. Shen, and Z. Chen, "Fully secure unidirectional identity-based proxy re-encryption," in *Proceedings of the 14th International Conference on Information Security and Cryptology*, 2011.

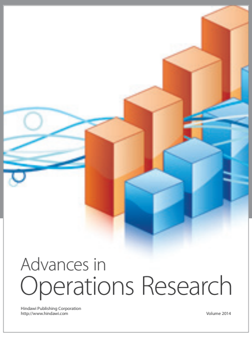
[28] A. Paul, J. C. Jiang, J. F. Wang, and J. F. Yang, "Parallel reconfigurable computing-based mapping algorithm for motion estimation in advanced video coding," *ACM Transaction on Embedded Computing Systems*, vol. 11, no. S2, article 40, 2012.

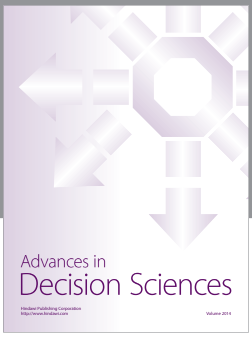
[29] A. Paul, "Dynamic power management for ubiquitous network devices," *Advanced Science Letters*, vol. 19, no. 7, pp. 2046–2049, 2013.

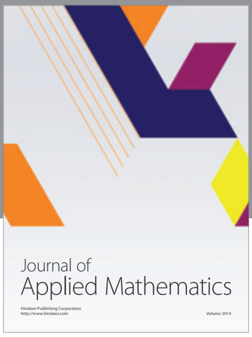
[30] A. Paul, "Graph based M2M Optimization in an IoT environment," in *Proceedings of the Research in Adaptive and Convergent Systems (ACM RACS '13)*, pp. 45–46, October 2013.

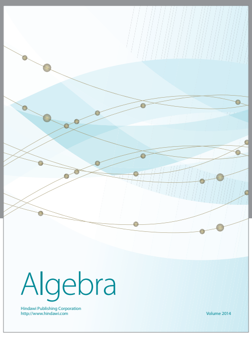
[31] D. G. Lee, J. Kim, J. Sung, Y. S. Lee, and S. Rho, "Cryptanalysis of block-wise stream ciphers suitable for the protection of multimedia and ubiquitous systems," *Telecommunication Systems*, vol. 44, no. 3-4, pp. 297–306, 2010.

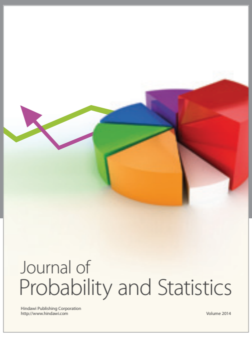
[32] S. Rho and S.-S. Yeo, "Bridging the semantic gap in multimedia emotion/mood recognition for ubiquitous computing environment," *Journal of Supercomputing*, vol. 56, no. 1, pp. 274–286, 2013.


Advances in
Operations Research

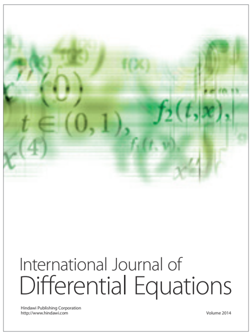

Advances in
Decision Sciences


Journal of
Applied Mathematics

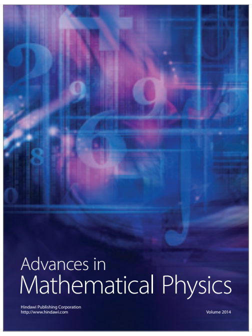

Algebra

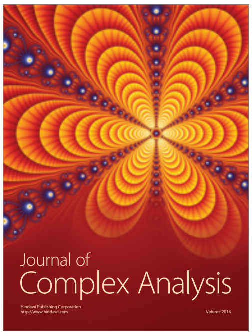

Journal of
Probability and Statistics

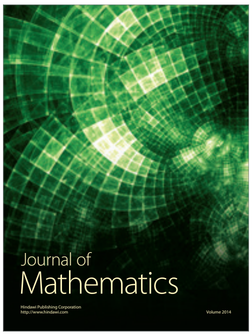
The Scientific
World Journal

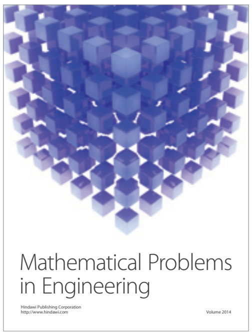

International Journal of
Differential Equations

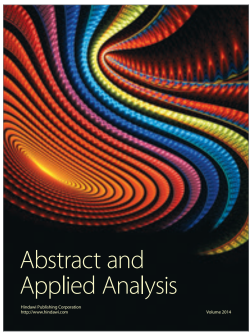
International Journal of
Combinatorics

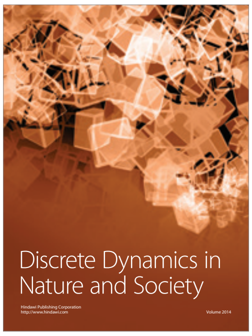

Advances in
Mathematical Physics

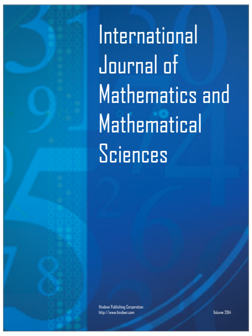

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

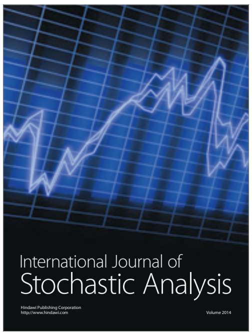

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization