Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(1): 53-60, Mar. 2012 **Regular Paper**

Attribute-based Proxy Re-encryption with a Constant Number of Pairing Operations

Hwa Jeong Seo, Howon Kim*, *Member, KIICE*

Department of Computer Engineering, Pusan National University, Pusan 609-735, Korea

Abstract

Attribute-based encryption (ABE) is an encryption scheme in which the user is able to decrypt a ciphertext with associated attributes. However, the scheme does not offer the capability of decryption to others when the user is offline. For this reason, the attribute-based proxy re-encryption (ABPRE) scheme was proposed, which combines traditional proxy re-encryption with ABE, so a user is able to empower designated users to decrypt the re-encrypted ciphertext with the associated attributes of designated users. However, previous ABPRE schemes demands a number of pairing operations that imply huge computational overhead. To reduce the number of pairing operations, we reduce the pairing operations with exponent operations. This paper provides a novel approach to an ABPRE scheme with constant pairing operation latency.

Index Terms: Attribute based encryption, Proxy re-encryption, Key delegation

I. INTRODUCTION

Identity-based cryptography encrypts the message with the user's identity including the name and e-mail address. An identity-based encryption (IBE) scheme can restrict an authority to indicate the identity of the recipient [1, 2]. Attribute-based encryption (ABE) was published by Sahai and Waters [3]. Unlike IBE, the message is encrypted with attributes, such as gender, age, and affiliation, so ABE schemes can designate the recipients by assigning common attributes of others. ABE consists of two policies. The first is the key policy ABE (KP-ABE) in which each private key is associated with an access structure [4]. The other scheme is the ciphertext policy ABE (CP-ABE), in which a ciphertext is associated with an access structure [5-7]. The attribute-based proxy re-encryption scheme (ABPRE) extends traditional proxy re-encryption to its attribute-based counterpart. Therefore, the capability of delegation is transferred to the designated users [8]. However, the previous ABPRE does not provide a constant length of message and number of pairing operations. Recently, a constant ciphertext length based CP-ABE was proposed by Emura et al. [9]. The computation cost and ciphertext length were reduced significantly compared to previous papers. However, the encryption scheme over ABPRE has not been proposed yet. For this reason, in the present paper, we propose a new constant computation-based ABPRE. The scheme utilizes the capability of delegation with constant pairing operations.

The rest of this paper is organized as follows. In section II, we describe ABPRE. In section III, preliminaries such as bilinear map and complexity assumptions are introduced to support the construction and the security proof. In section IV, our new ABPRE scheme is introduced and then we analyze security model and computation performance. Finally the conclusion is drawn in section V.

Received 23 September 2011, **Revised** 02 November 2011, **Accepted** 14 November 2011
***Corresponding Author** E-mail: howonkim@pusan.ac.kr

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.1.053** print ISSN:2234-8255 online ISSN:2234-8883

II. DEFINITION OF ABPRE

In ABPRE, a user can re-encrypt the ciphertext using a re-key. Detailed relationships are shown in Fig. 1. First U_1 generates the ciphertext C_1, which can be decrypted with U_1's attributes. One day, U_1 is absent, but we need to read the data from C_1. In this case, U_1 will store the re-encrypted ciphertext with attributes that represent the specific recipient or groups into a proxy-server. After that, U_2 can access to the proxy-server and then gain the re-encrypted data.

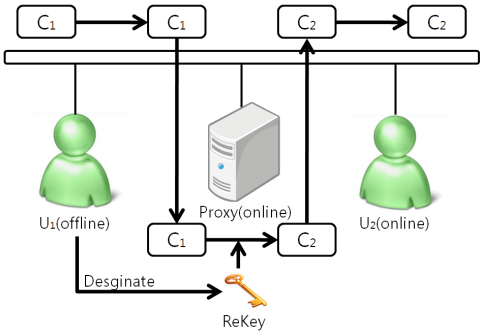

Fig 1. The attribute-based proxy re-encryption scheme system.

A. ABPRE Model

The ABPRE scheme is illustrated in [8, 10]. An ABPRE scheme is comprised of six steps including SETUP, KEYGEN, RE-GEN, ENC, RE-ENC, and DEC.

SETUP: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters pp and a master key mk.

KEYGEN (S, mk): The key generation algorithm takes as input the master key mk and a set of attributes S that describe the key. It outputs a private key usk.

RE-GEN (usk, AS): The re-key generation algorithm takes as input the secret key usk and access structure AS. It outputs a re-key rk.

ENC (m, AS): The encryption algorithm takes as input the public parameters pp, a message m, and an access structure AS over the universe of attributes. The algorithm will encrypt m and produce a ciphertext C such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. The ciphertext implicitly contains AS.

RE-ENC (rk, C): The re-encryption algorithm takes as input the re-key rk and a ciphertext C. First the algorithm checks the index set in rk. If rk satisfies the access structure of C, it outputs a re-encrypted ciphertext C'; otherwise, it rejects the re-key.

DEC (pp, C, usk): The decryption algorithm takes as input the public parameters pp, a ciphertext C, which contains an access policy AS, and a private key usk, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure AS then the algorithm will decrypt the ciphertext and return a message m.

III. PRELIMINARIES

In this section, some definitions which are the basis of attribute-based encryption schemes, including our scheme, are presented.

A. Bilinear Groups

Definition 1. Bilinear groups and a bilinear map are defined as follows: G and G_T are finite cyclic groups of prime order p. e is an efficiently computable bilinear map or pairing $e: G \times G \rightarrow G_T$, with the following properties;

Bilinearity: For any $g, h \in G$, and $a, b \in Z_p$, we have $e(g^a, h^b) = e(g, h)^{a \cdot b}$.

Non-degeneracy: $e(g, g) \neq 1$.

Note that $e(*,*)$ is symmetric since $e(g^a, g^b) = e(g, g)^{a \cdot b} = e(g^b, g^a)$.

B. Complexity Assumptions

Definition 2. Complex Triple Diffie-Hellman (CTDH) problem. Let $e: G \times G \rightarrow G_T$ be a bilinear map, where G has prime order p and g is a generator of G, random numbers $n, a, b, c, d, R \in Z_p$. Given a tuple

$$< g, n, g_b = g^b, g_c = g^c, g_d = g^d, g_1 = g^{\frac{c}{b}}, g_2 = g^{bc},$$

$$g_3 = g^{ac},$$

$$g_4 = g^{abc - Rc}, g_5 = g^{c(R+nd)}, g_6 = g^{\frac{c(R+nd)}{b}} >$$ as inputs, output g^{abc}.

Definition 3. Augment Diffie-Hellman (ADH) problem. Let $e: G \times G \rightarrow G_T$ be a bilinear map, where G has prime order p and g is a generator of G, random

numbers $a, b \in Z_p$. Given a tuple $< g, g^a, g^b, g^{b^2} >$ as inputs, output g^{ab}.

Definition 4. The CTDH assumption holds in G if no probabilistic polynomial time adversary is able to output g^{abc} from

$< g, n, g_b = g^b, g_c = g^c, g_d = g^d, g_1 = g^{\frac{c}{b}}, g_2 = g^{bc},$
$g_3 = g^{ac}, \quad g_4 = g^{abc-Rc},$
$g_5 = g^{c(R+nd)}, g_6 = g^{\frac{c(R+nd)}{b}} >$

with non-negligible advantage, where random numbers $n, a, b, c, d, R \in Z_p$ and generator $g \in G$ are chosen independently and uniformly at random.

The CTDH problem is more difficult than the ADH problem; if given the input of the ADH problem $< g, g^a, g^b, g^{b^2} >$, we could select $R + nd = 1, R = ab, b = c$ and outputs g^{Rc} from the CTDH oracle with inputs

$< g, n, g^c, g^c, g^{(1-R)n^{-1}}, g, g^{c^2}, g^R, 1, g^c, g >$.

The CTDH problem is the basis of the master key security in our scheme.

Definition 5. Augment decisional bilinear Diffie-Hellman (ADBDH) problem. Let $e : G \times G \to G_T$ be a bilinear map, where G has prime order p and g is a generator of G, random numbers $a, b, c \in Z_p$. Given a tuple $< g, A = g^a, B = g^b, C = g^c, B' = g^{\frac{1}{b}}, Z >$ as inputs, output 1 if $Z = e(g, g)^{abc}$; otherwise, output 0.

Definition 6. The ADBDH assumption holds in G if no probabilistic polynomial time adversary is able to distinguish the tuples

$D_{rand} =< g, g^a, g^b, g^c, g^{\frac{1}{b}}, e(g, g)^z >$ with non-negligible advantage, where $a, b, c, z \in Z_p$ and a generator $g \in G$ are chosen independently and uniformly at random.

IV. ATTRIBUTE-BASED PROXY RE-ENCRYPTION WITH CONSTANT PAIRING OPERATION LATENCY

A. Our Techniques

We adapt a constant number of pairing operations to a previous ABPRE scheme [8]. Whenever the attribute is decided in the scheme, to reflect the attributes, we need to compute the pairing operation with its designated attributes. To reduce the number of pairing operations, we reduce the pairing operation by using an exponential operation which can easily calculate the summation of the exponent. Therefore, we calculate the exponent and then compute the pairing operation just once.

B. Satisfying an Access Structure

In this scheme we consider the access structure consisting of AND gates between positive and negative attributes. Denote the index set of all the attributes as τ. The access structure is represented as $\wedge(+d_i, -d_i)_{i \in \tau}$, which are the positive attribute and the negative attribute, respectively. Any user receives a secret key associated with an attribute set $S \subseteq \tau$ from the authority. The users can decrypt the ciphertext, if the following conditions of the attribute are met:

If $+d_i$ appears in AS, then $i \in S$;

If $-d_i$ appears in AS, then $i \notin S$.

C. Main Construction

SETUP (1^k): A bilinear group G of prime order p, with bilinear map $e : G \times G \to G_T$ is generated. Next, it selects elements $k, y, z, t_i (1 \le i \le 3n)$ in Z_p and two generators g, h of G at random. Let $Y := e(g, h)^y$ and $T_i := g^{t_i}$ for each $1 \le i \le 3n$. The public parameter pp includes $< e, g^z, h, Y^{k \cdot z}, \{T_i, \frac{t_i}{k \cdot z}\}_{1 \le i \le 3n}, >$. The master key mk is $< k, y, z, \{t_i\}_{1 \le i \le 3n} >$.

KGEN (S, mk): Let S denote an index set of attributes. It chooses a random $r_1, \ldots, r_n$ from the Z_p and sets $r = r_1 + r_2 + \ldots + r_n$. It computes $\hat{D} = (h^{y-r})^k$, and for each $i \in N (N = \{1, 2, \ldots, n\})$: $(D_{i,1} = h^{r_i})_{i \in N}$. This outputs a user's secret key $usk =< S, (D_{i,1})_{i \in N}, \hat{D}, k \cdot z >$.

ENC (m, AS): Let AS denote an access structure. To encrypt a message $m \in G_T$, it selects a random $s \in Z_p$ and computes $\widetilde{C} = m \cdot Y^{s \cdot k \cdot z}$, $\hat{C} = g^{s \cdot z}$, $\breve{C} = h^{s \cdot k \cdot z}$. For $i \in N$: if $+d_i$ appears as AS, $C_i = T^{s}{}_i$; if $-d_i$ appears as AS, $C_i = T^{s}{}_{n+i}$; otherwise, $C_i = T^{s}{}_{2n+i}$. It outputs $C =< AS, \widetilde{C}, \hat{C}, \breve{C}, (C_i)_{i \in N} >$.

RKGEN (usk, AS'): Let usk denote a valid secret key consisting of $< S, (D_{i,1})_{i \in N}, \hat{D}, k \cdot z >$ and let AS' denote an access structure. It selects a random $d \in Z_p$ and set $\Im = g^d, \hat{D}' = \hat{D}$. For $i \in N \quad D'_{i,1} = D_{i,1} \cdot h^d$; C' is the

ciphertext of $\Im$ under the access structure AS'.

It outputs $rk =< S, AS', (D'_{i,1})_{i\in N}, \hat{D}', k\cdot z, C' >$

REENC(rk, C): Let rk denote a valid re-key consisting of $< S, AS', (D'_{i,1})_{i\in N}, \hat{D}', k\cdot z, C' >$ and C denote a well-formed ciphertext $< AS, \widetilde{C}, \hat{C}, \breve{C}, (C_i)_{i\in N} >$. This step checks whether S satisfies AS; if not, output $\perp$; otherwise, for $i \in N$:

$+d_i$ appears in AS, $T_i = \frac{t_i}{k\cdot z}$;

$-d_i$ appears in AS, $T_i = \frac{t_{n+i}}{k\cdot z}$.

Otherwise, $T_i = \frac{t_{2n+i}}{k\cdot z}$;

It computes $T = \frac{1}{\prod_{i\in N} T_i} = \frac{k\cdot z}{\sum_{j\in S} t_j} = \frac{k\cdot z}{t}$,

$C = \prod_{i\in N} C_i = g^{s\cdot\sum_{j\in S} t_j} = g^{s\cdot t}$ and

$D = \prod_{i\in N} D'_i = h^{d+\sum_{i\in N} r_i} = h^{n\cdot d+r}$.

Next it computes $E = e(C, D^T) = e(g,h)^{(n\cdot d+r)(k\cdot s\cdot z)}$.

It then computes

$\overline{C} = e(\hat{C}, \hat{D}')\cdot E = e(g^{s\cdot z}, h^{k\cdot(y-r)})\cdot e(g,h)^{(n\cdot d+r)(k\cdot s\cdot z)}$

$= e(g,h)^{(k\cdot s\cdot z\cdot y)+(n\cdot d\cdot k\cdot s\cdot z)}$;

It outputs a re-encrypted ciphertext

$C_{re} =< AS', \widetilde{C}, \overline{C}, \breve{C}, C' >$

Note that C_{re} can be re-encrypted iteratively. Thus we would obtain $C'_{re} =< AS'', \widetilde{C}, \overline{C}, \breve{C}, C'' >$ where C'' is obtained from the REENC algorithm with the input of another rk' and C'. The size of the ciphertext and re-encryption times increase linearly.

DEC (C, usk): Let usk denote a valid secret key $< S, (D_{i,1})_{i\in N}, \hat{D}, k\cdot z >$. It checks whether S satisfies AS; if not, it outputs $\perp$; otherwise, decrypt.

If C is an original well-formed ciphertext consisting of $< AS, \widetilde{C}, \hat{C}, \breve{C}, (C_i)_{i\in N} >$, for $i \in N$:

$+d_i$ appears in AS, $T_i = \frac{t_i}{k\cdot z}$;

$-d_i$ appears in AS, $T_i = \frac{t_{n+i}}{k\cdot z}$;

Otherwise, $T_i = \frac{t_{2n+i}}{k\cdot z}$.

It computes $T = \frac{1}{\prod_{i\in N} T_i} = \frac{k\cdot z}{\sum_{j\in S} t_j} = \frac{k\cdot z}{t}$,

$C = \prod_{i\in N} C_i = g^{s\cdot\sum_{j\in S} t_j} = g^{s\cdot t}$ and

$D = \prod_{i\in N} D_i = h^{\sum_{i\in N} r_i} = h^r$.

Next it computes $E = e(C, D^T) = e(g,h)^{k\cdot r\cdot s\cdot z}$.

It outputs

$$\frac{\widetilde{C}}{e(\hat{C},\hat{D})\cdot E} = \frac{m\cdot e(g,h)^{k\cdot s\cdot y\cdot z}}{e(g^{s\cdot z}, h^{(y-r)\cdot k})\cdot e(g,h)^{k\cdot r\cdot s\cdot z}} = m.$$

Otherwise, if C is a re-encrypted well-formed ciphertext consisting of $< AS', \widetilde{C}, \overline{C}, \breve{C}, C' >$, then it decrypts C' using usk and obtains $\Im = g^d$. Then it outputs $\frac{\widetilde{C}\cdot e(\Im, \breve{C})^n}{\overline{C}} = \frac{m\cdot e(g,h)^{k\cdot s\cdot y\cdot z}\cdot e(g,h)^{n\cdot d\cdot s\cdot k\cdot z}}{e(g,h)^{(k\cdot s\cdot z\cdot y)+(n\cdot d\cdot k\cdot s\cdot z)}} = m$.

Otherwise, if is a multi-time re-encrypted well-formed ciphertext, then decryption is similar with the above phases.

D. Security Proof for ABPRE

Since our scheme is an expansion of a previous ABPRE scheme in [8], the security proof is based on previous proof in [8] and we also extend it to our scheme.

Theorem 1: When the ADBDH assumption holds in (G, G_T), the ABPRE scheme ensures selective-structure chosen plaintext secure in the standard model.

Proof: In this section, we show that SS-CPA-ABPRE meets the requirements in terms of the ADBDH assumption.

We suppose that an adversary wins the SS-CPA-ABPRE game with a non-negligible advantage ε. A simulator S can be constructed to distinguish D_{adbdh} from D_{rand} with the non-negligible advantage $\frac{\varepsilon}{2}$.

We first suppose the challenger set the groups G and G_T with bilinear map e and a generator g. The challenger randomly selects a side of a fair coin c, without S 's intervention. If $c = true$ the challenger sets $< g, A, B, C, B', Z >\in D_{adbdh}$; otherwise it sets $< g, A, B, C, B', Z >\in D_{rand}$.

Init: S receives a challenge access structure AS^*, and names I_+^*, I_-^* the index set of positive and negative attributes, respectively. Then S chooses $x, y, \alpha_i, \beta_i, \gamma_i$ at random from Z_p for $i \in N$ and generates the public key $Y = e(A,B)^y$. Then S outputs the public parameters as follows:

$i \in I_+^*$, $T_i = g^{\alpha_i}, T_{n+i} = B^{\beta_i}, T_{2n+i} = B^{\gamma_i}$;

$i \in I_-^*$, $T_i = B^{\alpha_i}, T_{n+i} = g^{\beta_i}, T_{2n+i} = B^{\gamma_i}$;

Otherwise, $T_i = B^{\alpha_i}, T_{n+i} = B^{\beta_i}, T_{2n+i} = g^{\gamma_i}$.

Phase 1: An adversary A makes several queries to the key generation oracle O_{kg}, the re-key generation oracle O_{rkg}, and the re-encryption oracle O_{ree}.

A makes several queries to the O_{kg} with an index set I_q. According to the security game, if I_q satisfies AS^*, it outputs $\perp$.

Otherwise, S queries $usk =< I_q,(D_{i,1})_{i\in N},\hat{D},k\cdot z >$ from the oracle and outputs usk.

A makes a query to O_{rkg} with an index set I_q and an access structure AS. According to the security game, if I_q satisfies AS^*, it outputs $\perp$. Otherwise, S submits I_q to O_{kg} and obtains a secret key $usk =< I_q,(D_{i,1})_{i\in N},\hat{D},k\cdot z >$. S executes the following procedure:

It selects a random $d\in Z_p$ and set $\Im = g^d, \hat{D}' = \hat{D}$.

For $i\in N$ $D'_{i,1} = D_{i,1}\cdot h^d$,

it outputs $rk =< I_q, AS', (D'_{i,1})_{i\in N}, \hat{D}', k\cdot z, C' >$, in which C' is the ciphertext of $\Im$ under the access structure AS'.

A makes a query to O_{ree} with an index set I_q, an access structure AS', and a ciphertext $C =< AS,\widetilde{C},\hat{C},\breve{C},(C_i)_{i\in N} >$. According to the security game, if I_q satisfies AS^*, it outputs $\perp$. If I_q does not satisfy AS, it outputs $\perp$. Then S submits (I_q, AS') to the re-key generation oracle and obtains $rk =< I_q, AS', (D'_{i,1})_{i\in N}, \hat{D}', k\cdot z, C' >$. S uses rk to re-encrypt the ciphertext C. For $i\in N$:

$+d_i$ appears in AS, $T_i = \frac{t_i}{k\cdot z}$;

$-d_i$ appears in AS, $T_i = \frac{t_{n+i}}{k\cdot z}$;

Otherwise, $T_i = \frac{t_{2n+i}}{k\cdot z}$.

It computes $T = \frac{1}{\prod_{i\in N} T_i} = \frac{k\cdot z}{\sum_{j\in S} t_j} = \frac{k\cdot z}{t}$,

$C = \prod_{i\in N} C_i = g^{s\cdot\sum_{j\in S} t_j} = g^{s\cdot t}$, and

$D = \prod_{i\in N} D'_i = h^{d+\sum_{i\in N} r_i} = h^{n\cdot d+r}$. Next, it computes

$E = e(C, D^T) = e(g,h)^{(n\cdot d+r)(k\cdot s\cdot z)}$.

Finally, it computes

$\overline{C} = e(\hat{C}^{k\cdot z}, \hat{D}')\cdot E = e(g^{k\cdot s\cdot z}, h^{y-r})\cdot e(g,h)^{(n\cdot d+r)(k\cdot s\cdot z)}$

$= e(g,h)^{(k\cdot s\cdot z\cdot y)+(n\cdot d\cdot k\cdot s\cdot z)}$; It outputs a re-encrypted ciphertext $C_{re} =< AS', \widetilde{C}, \overline{C}, \breve{C}, C' >$.

Challenge: A submits two equal messages M_0 and M_1 in length. S produces a challenge ciphertext:

$C^* =< \widetilde{C} = M_\mu\cdot Z^k, C, C^k, (C^{\alpha_i})_{i\in I_+{}^*}, (C^{\beta_i})_{i\in I_-{}^*}, (C^{\gamma_i})_{i\notin I_+{}^*\cup I_-{}^*} >$.

Phase 2: Same procedure as Phase 1.

Guess: A tuple was given from D_{adbdh} when S outputs $c' = 1$ and A gives a correct guess $\mu' = \mu$; otherwise a tuple was given from D_{rand} when S outputs $c' = 0$.

According to [3], the advantage of the simulator to output a correct $v' = v$ is $\Pr[v = v'] - \frac{1}{2}$

$= \Pr[v = v', v = 0] + \Pr[v = v', v = 1] - \frac{1}{2} = \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot(\frac{1}{2}+\varepsilon) - \frac{1}{2} = \frac{\varepsilon}{2}$

Theorem 2: If the CTDH assumption holds in G, G_T, then the ABPRE scheme has master key security.

Proof: The simulator S receives a tuple

$< g, n, g_b = g^b, h = g^c, g_d = g^d, g_1 = g^{\frac{c}{b}}, g_2 = g^{bc},$

$g_3 = g^{ac}$, $g_4 = g^{abc-Rc}$,

$g_5 = g^{c(R+nd)}, g_6 = g^{\frac{c(R+nd)}{b}} >$ and a challenge index set I^*. To output g^{abc}, the simulator S does as follows:

Init: S chooses $\alpha_i, \beta_i, \gamma_i$ at random from Z_p for $i\in N$ and generates the public key and set $Y = e(g,h)^{ab} = e(g_b, g_3)$. Then it computes public keys as follows:

$i\in I^*$, $T_i = g^{\alpha_i}, T_{n+i} = g_b{}^{\beta_i}, T_{2n+i} = g_b{}^{\gamma_i}$;

$i\notin I^*$, $T_i = g_b{}^{\alpha_i}, T_{n+i} = g^{\beta_i}, T_{2n+i} = g_b{}^{\gamma_i}$.

S outputs public parameter

$pp :=< e, g^z, h, Y^{k\cdot z}, \{T_i, T_{n+i}, T_{2n+i}, \frac{t_i}{k\cdot z}\}_{i\in N} >$.

Key generation oracle: A makes a query to the key generation oracle with an index set $I_q\subseteq N$ where $I_q\neq I^*$. An index j must belong to the following conditions $((j\in I_q)\wedge(j\notin I^*)$ or $(j\notin I_q)\wedge(j\in I^*))$. For this reason, we just analyze the case of $(j\notin I_q)\wedge(j\in I^*)$.

For every $i\in N, S$ chooses $r'_i\in Z_p$ at random and implicitly sets r_i in the following ways: $r_i = br'_i$ $(i\neq j;)$, $r_j = ab + br'_i$ (otherwise).

Denote $r = \sum_{i=1}^n r_i = ab + \sum_{i=1}^n r'_i\cdot b$ and

$\hat{D} = (h^{y-r})^k = h^{k(-\sum_{i=1}^n r'_i\cdot b)} = \prod_{i=1}^n g_2{}^{\frac{k}{r'_i}}$.

For $i\in I_q$, $i\neq j$: if $i\in I^*$ $D_{i,1} = D_{i,2} = h^{r_i} = g_2{}^{r'_i}$

else $i\notin I^*$ $D_{i,1} = D_{i,2} = h^{r_i} = g_2{}^{r'_i}$.

For $i\notin I_q$, $i = j$: if $i\in I^*$, $D_{i,1} = D_{i,2} = h^{r_i} = g_2{}^{r'_i}$

else $i\notin I^*$ $D_{i,1} = D_{i,2} = h^{r_i} = g_2{}^{r'_i}$.

For, $i = j$: , $D_{i,1} = D_{i,2} = h^{r_i} = h^{ab+br'}$.

It outputs a secret key $usk =< I_q, (D_{i,1})_{i \in N}, \hat{D}, k \cdot z >$.

Rekey generation oracle: A makes a query to the key generation oracle with an index set $I_q \subseteq N$ and access structure AS , if $I_q \neq I^*.$, obtain usk from $KGEN(I_q)$ and generate $rk = RKGEN(usk, AS)$; else $I_q = I^*$.

Select $j \in I^*$ and $r_i', r \in Z_p$ at random for each $i \in N \setminus \{j\}$;

Implicitly set $r_j' = r + R + nd - \sum_{i=1, i \neq j}^{n} r_i'$ and $r_i = r_i' - d$ for $i \in N$;

Compute

$\hat{D}' = h^{k(y - \sum_{i=1}^{n} r_i)} = h^{k(y - \sum_{i=1}^{n} (r_i' - d))} = h^{k(ab - R - r)} = (g_4 h^{-r})^k$;

For $i \in N$:

If $i \neq j, i \in I^*, D_{i,1}' = h^{r_i + d} = h^{r_i'}$;

Else if $i \neq j, i \notin I^*, D_{i,1}' = h^{r_i + d} = h^{r_i'}$;

Else if

$i = j, D_{i,1}' = h^{r_j + d} = h^{r_j'} = h^{r + R + nd - \sum_{i=1, i \neq j}^{n} r_i'} = g_5 h^{r - \sum_{i=1, i \neq j}^{n} r_i'}$

Output $rk =< S, AS', (D_{i,1}')_{i \in N}, \hat{D}', k \cdot z, C' >$ where C is the ciphertext of $g_d \cdot g^t$ under the access structure AS .

Re-encryption oracle: A makes a query to the key generation oracle with an index set $I_q \subseteq N$ and access structure: if $I_q \neq I^*.$, obtain rk from $RKGEN(usk, AS')$ and generate $C' = REENC(rk, C)$; else $I_q = I^*$.

-For $i \in N$:

- $+d_i$ appears in AS , $D_{i,1}'^{T_i} = h^{\frac{r_i + d}{kz\alpha_i}} = h^{\frac{r_i'}{kz\alpha_i}}$ where $T_i = \frac{t_i}{k \cdot z}$;

- $-d_i$ appears in AS , $D_{i,1}'^{T_i} = h^{\frac{r_i + d}{kz\beta_i}} = h^{\frac{r_i'}{kz\beta_i}}$ where $T_i = \frac{t_{n+i}}{k \cdot z}$;

- Otherwise, $D_{i,2}'^{T_i} = h^{\frac{r_i + d}{bkz\gamma_i}} = h^{\frac{r_i'}{kz\gamma_i}}$ where $T_i = \frac{t_{2n+i}}{k \cdot z}$.

It outputs a secret key usk^* for I^* including $usk =< S, (D_{i,1})_{i \in N}, \hat{D}, k \cdot z >$. If it is a valid secret key, usk^* satisfies the following equation: $e(g^z, \hat{D}) \prod_{i \in I^*} e(T_i, D_{i,1}^T) \prod_{i \notin I^*} e(T_{n+i}, D_{i,1}^T) = e(g, h)^y$;

The decryption oracle is straightforward, since the secret key and re-key could be correctly generated from the Key generation and Rekey generation oracle.

It outputs $\hat{D}^z \cdot \prod_{i \in I^*} D_{i,1}^{T \cdot \alpha_i} \cdot \prod_{i \in I^*} D_{i,1}^{T \cdot \beta_i} = h^y = g^{abc}$ and solves the CTDH problem.

E. Evaluation

Majority of ABE or ABPRE schemes require computing a number of pairing operations to generate the ciphertext depending on unique attributes but the computational cost of a pairing operation is much higher than other operations. For this reason, a small number of pairing operations is important factor for efficient cryptography algorithms. In 2009, Emura et al. [9] presented a constant length of pairing operations in an ABE scheme. This scheme is the motivation of our algorithm. In our scheme, we propose an expansion algorithm of ABE, ABPRE maintaining a constant pairing operation. A comparison of computation complexity is illustrated in Table 1.

The notation kG and kC_e denote the k-times calculation over group G and pairing, respectively. Let $u = \{att_1, att_2, \ldots, att_n\}$ be the set of attributes.

Table 1. Computational time of each algorithm

	Encryption	Decryption	Re-encryption	Re-encrypted decryption
Cheung & Newport [5]	$(n+1)G_1 + 2G_T$	$(n+1)C_e + (n+1)G_T$	-	-
Bethencourt et al. [7]	$(2r_1+1)G_1 + 2G_T$	$2r_1C_e + (2r_1+2)G_T$	-	-
Nishide et al. [11]	$(2N'+1)G_1 + 2G_T$	$(3n+1)C_e + (3n+1)G_T$	-	-
Waters [12]	$(1+3r_1n)G_1 + 2G_T$	$(1+n+r_1)C_e + (3r_1-1)G_1 + 3G_T$	-	-
Emura et al. [9]	$(n+1)G_1 + 2G_T$	$2C_e + 2G_T$	-	-
Liang et al. [8]	$(n+2)G_1 + 2G_T$	$2G_T + (n+2)C_e$	$G_T + (n+1)C_e$	$4G_T + (n+3)C_e$
Our scheme	$(n+2)G_1 + 2G_T$	$(3n+2)G_1 + 2G_T + 2C_e$	$3nG_1 + G_T + 2C_e$	$3nG_1 + 4G_T + 3C_e$

Table 2. Some properties of attribute-based encryption schemes

	Policy	Recipient anonymity	Capability of delegation	Assumption
Cheung & Newport [5]	Ciphertext	No	No	DBDH
Bethencourt et al. [7]	Ciphertext	No	No	Generic group model
Nishide et al. [11]	Ciphertext	Yes	No	DBDH, D-linear
Waters [12]	Ciphertext	No	No	DBDH
Emura et al. [9]	Ciphertext	No	No	DBDH
Liang et al. [8]	Ciphertext	No	Yes	CTDH, ADBDH
Our scheme	Ciphertext	No	Yes	CTDH, ADBDH

DBDH: decisional bilinear Diffie-Hellman, CTDH: complex triple Diffie-Hellman, ADBDH: augment decisional bilinear Diffie-Hellman.

Let r_1 and r_2 be a set of attributes associated with the ciphert

ext and a set of attributes associated with the secret key, respectively. Let $N^{/=\sum_{i=1}^{n} n_i}$ be the total number of possible statements of attributes.

Comparison of some properties including policy anonymity, capability of delegation, and security assumption is illustrated in Table 2. All schemes follow the ciphertext policy. Nishide et al. [11] scheme only provides recipient anonymity. Capability of delegation is a strong feature of ABPRE-based schemes. Therefore, we can empower designated users with the capability of decryption. Our security assumption is based on CTDH and ADBDH. This provides a selective-structure chosen to be plaintext secure and master key secure.

V. CONCLUSIONS

In the paper, we present the ABPRE with constant number of pairing operations. The scheme is motivated from previous CP-ABE by computing constant length and number of pairing operations. Compared to previous ones, our proposal has the strength of its capability of delegation. Through the feature, we can empower designated users to decrypt the ciphertext re-encrypted with a new access structure. The scheme can be adapted to various applications including e-mail forwarding and distributed file systems.

Future work includes how to implement the scheme efficiently in various environments such as traditional computing environments and embedded systems (wireless sensor network, near field communication, and radio frequency identification).

ACKNOWLEDGMENTS

This work was supported for two years by a Pusan National University Research grant.

REFERENCES

[1] D. Boneh and M. K. Franklin, “Identity-based encryption from the weil pairing,” *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara: CA, pp. 213-229, 2001.

[2] X. Boyen and B. Waters, “Anonymous hierarchical identity-based encryption,” *Proceedings of the 26th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara: CA, pp. 290-307, 2006.

[3] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, pp. 457-473, 2005.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria: VA, pp. 89-98, 2006.

[5] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” *Proceedings of the 14th ACM conference on Computer and Communications Security*, Alexandria: VA, pp. 456-465, 2007.

[6] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” *Proceedings of the 35th international colloquium on Automata, Languages and Programming*, Reykjavik, Iceland, pp. 579-591, 2008.

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Oakland: CA, pp. 321-334, 2007.

[8] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy re-encryption with delegating capabilities,” *Proceedings of the 4th*

International Symposium on Information, Computer, and Communications Security, Sidney, Australia, pp. 276–286, 2009.

[9] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext policy attribute-based encryption scheme with constant ciphertext length," *Proceedings of the 5th International Conference on Information Security Practice and Experience*, Shaanxi, China, pp. 13-23, 2009.

[10] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," *Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandria: VA, pp. 185-194, 2007.

[11] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," *Proceedings of the 6th International Conference on Applied Cryptography and Network Security*, New York: NY, pp. 111-129, 2008.

[12] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography*, Taormina, Italy, pp. 53-70, 2008.

Hwajeong Seo

He received the BSEE degree from Pusan National University, Pusan, Republic of Korea in 2010, and he is in the MS degree program in Computer Engineering at Pusan National University. His research interests include sensor networks, information security, Elliptic Curve Cryptography, and RFID security. He is a member of IEEE.

Howon Kim

He received the BSEE degree from Kyungpook National University, Daegu, Republic of Korea, in 1993 and the MS and PhD degrees in electronic and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of the technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently working as an associate professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Republic of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems, and their security issues. He is a member of the IEEE, and the International Association for Cryptologic Research (IACR).