Hybrid Proxy Re-encryption Scheme for Attribute-Based Encryption

Takeo Mizuno[1,2] and Hiroshi Doi[2]

[1] NTT DATA CORPORATION, 3-3-3 Toyosu, Koutou-ku, Tokyo, 135-6033 Japan
[2] INSTITUTE of INFORMATION SECURITY, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 221-0835 Japan
mizunotko@nttdata.co.jp, doi@iisec.ac.jp

Abstract. In ciphertext policy *attribute based encryption* (ABE) schemes the sender selects an access structure and generates a ciphertext, which decryptors can get plaintext if he has certain set of secret key associate with his attributes which satisfies the access structure. On the other hand, many organisations already introduced standard *identity based encryption* (IBE) or *public key encryption* (PKE) where only a single recipient is specified at the time of encryption. To utilize the above schemes and to simplify the management of user's key, it is valuable to develop a proxy re-encryption schemes between ABE schemes and IBE schemes. In this paper we propose the first proxy re-encryption scheme, which can convert an ABE ciphertext to a ciphertext which is encrypted by IBE scheme. Using new proxy re-encryption scheme, some useful applications can be constructed. Furthermore, we prove the security in the standard model based on decisional bilinear Diffie-Hellman assumption.

Keywords: attribute-based encryption, proxy re-encryption, identity-based encryption, bilinear maps.

1 Introduction

In ciphertext policy *attribute based encryption* (ABE) schemes the sender selects an access structure and generates a ciphertext, which decryptors can get plaintext if he has certain set of secret key associate with his attributes which satisfies the access structure. Using the ABE scheme, the sender does not specify all the recipients at the time of encryption, and enforces access policies, defined on attributes within the encryption procedure.

Suppose some organisation plan to apply an ABE scheme to share the secret data among members securely. They might have been applied *identity based encryption* (IBE) or *public key encryption* (PKE) system, where only a single recipient is specified at the time of encryption, already. If they plan to distribute the ABE secret keys to the members, the ABE key authority should generates ABE secret keys to each members, and the member should manage the ABE secret key in addition.

On the other hand, in proxy re-encryption schemes, a semi-trusted entity called proxy can convert a ciphertext encrypted for Alice into a new ciphertext,

F. Bao et al. (Eds.): Inscrypt 2009, LNCS 6151, pp. 288–302, 2010.

which another user Bob can decrypt with his own secret information without revealing the underlying plaintext. Because the proxy is not fully trusted, it is required that the proxy cannot reveal Alice's and Bob's secret key, and cannot learn the plaintext during the conversion. If the proxy which can convert the ABE ciphertext to the IBE ciphertext exists, the IBE user can decrypt the ABE ciphertext using his own IBE secret key only. In this paper, we propose the first proxy re-encryption scheme which can convert the ABE ciphertext to the IBE ciphertext securely.

If the above mentioned organisation builds the gateway which converts ABE ciphertexts to IBE ciphertext with our new proxy re-encryption scheme, the member of the organization can access ABE ciphertexts only using this gateway, and stores IBE secret key only. This gateway only re-encrypts ABE ciphertext to IBE ciphertext without revealing underling plaintext.

Furthermore, the member of the organisation does not need to consider about decryption operation of the ABE scheme. The proxy removes the effect of the ABE scheme.

1.1 Attribute-Based Encryption Schemes

The ABE schemes were first introduced by Sahai and Waters as an application of their fuzzy IBE scheme [2], which have single threshold access structure.

Two variants of ABE were subsequently proposed. The key policy attribute-based encryption (KP-ABE) was proposed by Goyal, Pandey, Sahai and Waters in [22]. In [22], every ciphertext are associated with a set of attributes, and every user's secret key is associated with a monotone access structure on attributes. Decryption is enabled iff the ciphertext attribute set satisfies the access structure on the user's secret key. The first ciphertext policy attribute-based encryption (CP-ABE) was proposed by Bethencourt, Sahai and Waters in [11]. In [11], the situation is reversed: attributes are associated with user's secret keys and monotone access structures with ciphertexts. However, in [11], the security of scheme was proved in generic bilinear group model only. Cheung and Newport proposed a simple and provably secure CP-ABE scheme in standard model, where the access policy is defined by AND gates, in [12]. Waters [5] recently proposed the first fully expressive CP-ABE in the standard model.

1.2 Proxy Re-encryption Schemes

Several proxy re-encryption schemes have been proposed in the context of *public key encryption* (PKE), e.g., ElGamal or RSA. Other schemes have been proposed in the context of *identity based encryption* (IBE) which the sender encrypts a plaintext using arbitral strings that represents the recipient's identity as the public key.

Matsuo proposed a hybrid proxy re-encryption scheme which can convert a PKE ciphertext to an IBE chiphertext in [20]. He also classifies proxy re-encryption schemes as follows:

[PKE-PKE] type Proxy converts PKE ciphertexts to PKE ciphertexts. [17], [14], [16], [23], [13], [10], [18], [9] and [3] have been proposed as this type.
[IBE-IBE] type Proxy converts IBE ciphertexts to IBE ciphertexts. [23], [20], [15], and [6] have been proposed as this type.
[PKE-IBE] type Proxy converts PKE ciphertexts to IBE ciphertexts. [20] has been proposed as this type.
[IBE-PKE] type Proxy converts IBE ciphertexts to PKE ciphertexts. [15] [21] have been proposed as this type.

1.3 Our Contribution

We propose [ABE-IBE] type proxy re-encryption scheme, which can convert a ciphertext encrypted by ABE scheme to an IBE ciphertext, without revealing the underlying plaintext. Our scheme holds the following advantages simultaneously.

- Our scheme achieve proxy invisibility, which means delegatee does not require additional algorithm and does not require additional secret information while decrypting a re-encrypted ciphertext.
- In our scheme the size of a re-encrypted ciphertext is same as an original ABE ciphertext, while in some scheme ([15]) requires additional elements of ciphertext only used for re-encryption.
- Our scheme are secure in the standard model against chosen plaintext attack. We prove the security, combining two different scheme (ABE and IBE) all together.

1.4 Organisation

The rest of paper consists of 4 sections. In section 2 we give some definitions and preliminaries. In section 3 we define security of [ABE-IBE] type proxy re-encryption. In section 6 we give an extension of our scheme. In section 4 we present the [ABE-IBE] type proxy re-encryption scheme, in section 5 we prove the security, and finally conclude this study in section 7.

2 Preliminaries

2.1 Bilinear Groups

Let $\mathbb{G}$, $\mathbb{G}_T$ be the two multiplicative cyclic groups of prime order p, and g be a generator of $\mathbb{G}$. We say that $\mathbb{G}_T$ has an admissible bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ if the following conditions hold.

1. $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for all a, b
2. $\hat{e}(g, g) \neq 1$

We say that $\mathbb{G}$ is a bilinear group if the group action in $\mathbb{G}$ can be computed efficiently and there exists a group $\mathbb{G}_T$ and an efficiently computable bilinear map $\hat{e}$ as above.

2.2 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

The Decisional BDH problem [1], [19], [7] in $\mathbb{G}$ is defined as follows:

The challenger chooses $a, b, c \in \mathbb{Z}_p$ at random and then flips a fair binary coin β. If $\beta = 1$ it outputs the tuple $\left\langle g, g^a, g^b, g^c, \hat{e}\left(g,g\right)^{abc} \right\rangle \in \mathbb{G}^4 \times \mathbb{G}_T$. Otherwise, if $\beta = 0$, the challenger choose $\Gamma_T \in_R \mathbb{G}_T$ at random and outputs the tuple $\left\langle g, g^a, g^b, g^c, \Gamma_T \right\rangle \in \mathbb{G}^4 \times \mathbb{G}_T$. The adversary must then output a guess β' of β. An adversary, $\mathcal{B}$, has at least an ϵ advantage in solving the decisional DBDH problem if $\left|\Pr\left[\beta = \beta'\right] - \frac{1}{2}\right| \geq \epsilon$ where the probability is taken over the random choice of the generator g, the random choice of a, b, c in $\mathbb{Z}_p$ and Γ_T in $\mathbb{G}_T$, and the random bits consumed by $\mathcal{B}$.

Definition 1. *The Decisional (κ, t, ϵ)-BDH assumption holds in $\mathbb{G}$ if no t-time adversary has at least ϵ advantage in solving the Decisional BDH problem in $\mathbb{G}$ under a security parameter κ.*

2.3 Ciphertext Policy ABE

The access structure on attribute is a rule W that returns either 0 or 1 given a set S of attributes. We say that S satisfies W(written $S \models W$) if and only if W answers 1 on S. In ABE schemes, access structures may be Boolean expressions, threshold trees, etc. A ciphertext policy attribute based encryption (ABE) consists of the following algorithms.

$SetUp_A(1^\kappa)$ Given a security parameter 1^κ as input, outputs a public key PK_A and master secret key MK_A.

$KeyGen_A(MK_A, S)$ Let $\mathcal{N}$ be the set of all attributes in the system. For input of a master secret key MK_A, and a set $S \in \mathcal{N}$ of attributes, outputs a secret key SK_A associated with S.

$Encrypt_A(PK_A, M, W)$ For input of a public key PK_A, a message M and an access structure W, outputs a ciphertext C_A with the property that a user with a secret key generated from attribute set S can decrypt C_A iff $S \models W$.

$Decrypt_A(C_A, SK_A)$ For input of a ciphertext C_A and a secret key SK_A, outputs the message M if $S \models W$, where S is the attribute set used to generate SK_A.

2.4 Identity Based Encryption

Identity Based Encryption (IBE) consists of the following algorithm.

$SetUp_I(1^\kappa)$ Given a security parameter 1^κ as input, a trusted entity called Private Key Generator (PKG) generates a master key MK_I and public parameters π, and outputs MK_I and π.

$KeyGen_I(MK_I, \pi, ID)$ For inputs of a master key MK_I, public parameters π, and an identity ID, the PKG outputs an IBE secret key SK_I corresponding to the identity.

$Enc_I(ID, \pi, M)$ For inputs of an identity ID, public parameters π, and a plaintext M, outputs an IBE ciphertext C_I.

$Dec_I(SK_I, \pi, C_I)$ For inputs of a IBE secret key SK_I, public parameters π, and an IBE ciphertext C_I, decrypts a plaintext M.

2.5 [ABE-IBE] Proxy Re-encryption

The [ABE-IBE] type proxy re-encryption consists of the following algorithms.

$KenGen_{A \to I}(S, ID, s_{ID}, SK_A, \pi)$ For inputs of a set of attributes S, an IBE identity ID, IBE public parameter π, an IBE additional secret information to generate re-encryption key s_{ID}, and an ABE secret key SK_A, outputs a re-encrypt key $RK_{A \to I}$ to the proxy.

$ReEncrypt_{A \to I}(RK_{A \to I}, C_A)$ For inputs of a re-encrypt key $RK_{A \to I}$ and an ABE ciphertext C_A, the proxy re-encrypts and outputs a IBE ciphertext C_I to the delegatee.

3 Chosen Plaintext Security for [ABE-IBE] Type Proxy Re-encryption

We define chosen plaintext security for [ABE-IBE] type proxy re-encryption scheme according to the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

We design the following game on the basis of Cheung and Newport's CPA Security Game for ABE in [12], Boneh and Boyen's selective ID game in [8] and Green and Ateniese's proxy re-encryption game [15]. We show even if an adversary obtains additional informations related to proxy re-encryption, such as re-encryption keys, they does not affect the security of underlying ABE and IBE scheme. In the challenge phase, the adversary can adaptively select which scheme to attack (ABE or IBE), this implies that these two schemes which are combined by our scheme, secure against chosen plaintext attacks.

In the following game, the adversary is allowed to adaptively conduct ABE secret key queries, IBE secret key queries and re-encryption key queries. Following the claim of Green and Ateniese, the adversary must not be restricted to obtain re-encryption keys which can convert the target ciphertext to a ciphertext if the adversary cannot decrypt it, in [15]. In other words, the adversary was only restricted to obtain the set of secret keys which can decrypt the target ciphertext.

Hence, in our security definition, the adversary is restricted to obtain re-encryption keys which can convert a target ABE ciphertext to an identity whose IBE secret key is already queried (and answered). In this case, the adversary can convert the target ABE ciphertext to a ciphertext which can be decrypted by the IBE key which is the adversary already obtains. The adversary is also restricted to obtain an IBE secret key, if the adversary already obtain re-encryption key which can convert the target ABE ciphertext to that identity.

Definition 2. *(Security of [ABE-IBE] type proxy re-encryption) The security against [ABE-IBE] type proxy re-encryption scheme is defined according to the following game between an attacker $\mathcal{A}$ and a challenger $\mathcal{C}$.*

Init : $\mathcal{A}$ chooses the following and sends them to $\mathcal{C}$.
- The target access structure W.
- The target IBE identity ID^*.

SetUp : $\mathcal{C}$ runs the $Setup_A(1^\kappa)$ and $Setup_I(1^\kappa)$. $\mathcal{C}$ gives ABE public parameters and IBE public parameters to the $\mathcal{A}$.

Phase 1 :

$Extract_A(S)$: $\mathcal{A}$ can adaptively request an ABE secret key for a set S where $S \not\models W$. $\mathcal{A}$ can repeat this multiple times.

$Extract_I(ID, params)$: $\mathcal{A}$ can adaptively request an IBE secret key corresponding to an identity ID of his choice. $\mathcal{A}$ can repeat this multiple times for different IBE identities.

$Extract_{A\to I}(S, ID)$: $\mathcal{A}$ can adaptively request re-encryption key which can transform ABE ciphertexts encrypted for set S to IBE ciphertexts corresponding to an identity ID. $\mathcal{A}$ can repeat this multiple times for different sets and identities.

Challenge : $\mathcal{A}$ submits two equal length messages M_0 and M_1 and selects which scheme to attack(ABE or IBE). $\mathcal{C}$ flips a coin $\mu \in \{0, 1\}$ and returns the encrypted result of M_μ encrypted by the selected scheme.

Phase 2 : Same as Phase 1.

Solve : $\mathcal{A}$ submits a guess $\mu' \in \{0, 1\}$ for μ. The adversary $\mathcal{A}$ wins if $\mu' = \mu$.

During Phase 1 and 2, $\mathcal{A}$ is restricted the following queries which $\mathcal{A}$ can decrypt a challenge ciphertext only using $\mathcal{C}$'s answers

- $Extract_A(S^*)$, where $S^* \models W$.
- $Extract_I(ID^*)$.
- The set of queries $Extract_{A\to I}(S^*, ID)$ and $Extract_I(ID, param)$, where $S^* \models W$ and ID is an identity of IBE user.

Definition 3. *Let $\mathcal{A}$ be an adversary against our scheme. We define the IND-sAttr-CPA advantage of $\mathcal{A}$ is $Adv_{\mathcal{A}}(\kappa) = 2(\Pr[\mu' = \mu] - 1/2)$.*

We say that the our scheme is (κ, t, q, ϵ) adaptive chosen plaintext secure if for any t-time adversary $\mathcal{A}$ that makes at most q chosen queries under a security parameter κ, we have that $Adv_{\mathcal{A}}(\kappa) < \epsilon$.

4 Construction

We construct an [ABE-IBE] type proxy re-encryption scheme which achieves CPA-security without random oracle.

Our scheme enables conversion of an ABE ciphertext to an IBE ciphertext. Our construction is based on Basic Construction of Cheung and Newport ABE scheme proposed in [12], because [12] is proved DBDH assumption and we combine the security of ABE and IBE schemes which bridged by our re-encryption method under single assumption. Furthermore, we use [8] as IBE scheme which achieves selective ID security under DBDH assumption.

4.1 CN-ABE Scheme

Let the set of attributes $\mathcal{N} = \{1, \cdots, n\}$ for some natural number n. We refer to attributes i and their negations $\neg i$ as *literals*. In [12], access structure consists of a single *AND* gate whose input are literals and denoted as $\bigwedge_{i \in I} \underline{i}$, where $I \subseteq \mathcal{N}$ and every $\underline{i}$ is a literal(i.e. i or $\neg i$).

$SetUp_A(1^\kappa)$ Let $\mathbb{G}, \mathbb{G}_T$ be a bilinear group of prime order p. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map. Choose a random generator $g \in \mathbb{G}$ and $t_0, t_1, \cdots, t_{3n} \in_R \mathbb{Z}_p$. Let $T_0 = \hat{e}(g,g)^{t_0}$ and $T_j = g^{t_j}$ for each $j \in \{1, \cdots, 3n\}$. The public key is $PK_A = \langle \hat{e}, g, T_0, T_1, \cdots T_{3n} \rangle$. The master secret key is $MK_A = \langle t_0, t_1, \cdots, t_{3n} \rangle$.
The public key element T_i, T_{n+i} and T_{2n+i} correspond to the three types of occurrences of i: positive, $n+i$: negative and $2n+i$: *don't care* for each $i \in \{1, \cdots, n\}$.

$Encrypt_A(M, W)$ Given a message $M \in \mathbb{G}_T$ and an *AND* gate $W = \bigwedge_{i \in I} \underline{i}$ as input, select a random element $s \in \mathbb{Z}_p$ and sets $\widetilde{C} = M \cdot T_0^s$ and $\widehat{C} = g^s$. For each $i \in I$, set C_i as follows: If $i \in I$ and $\underline{i} = i$, set $C_i = T_i^s$. If $i \in I$ and $\underline{i} = \neg i$, set $C_i = T_{n+i}^s$. For each $i \in \mathcal{N} \setminus I$, set $C_i = T_{2n+i}^s$. The ciphertext is $C_A = \left\langle W, \widetilde{C}, \widehat{C}, \{C_i | i \in \mathcal{N}\} \right\rangle$.

$KeyGen_A(S, MK_A)$ Given the attribute set S and ABE master secret key MK_A as input, output a secret key $SK_A = \left\langle \widehat{D}, \{\langle D_i, F_i \rangle | i \in \mathcal{N}\} \right\rangle$ as follows:
Select $r_i \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$ and set $r = \sum_{i=1}^n r_i$.

1. Set $\widehat{D} = g^{t_0 - r}$.
2. For each $i \in \mathcal{N}$, set D_i as follows:
   If $i \in S$, set $D_i = g^{\frac{r_i}{t_i}}$. If $i \notin S$, set $D_i = g^{\frac{r_i}{t_{n+i}}}$. Note that every $i \in S$ represents a positive attribute and $i \notin S$ represents a negative attribute.
3. For every $i \in \mathcal{N}$, set $F_i = g^{\frac{r_i}{t_{2n+i}}}$.

$Decrypt_A(SK_A, C_A)$ Given an ABE secret key SK_A and an ABE ciphertext C_A as input, if an ABE secret key SK_A can satisfy *AND* gate W in the ABE ciphertext C_A, output a plaintext as follows:

1. For each $i \in \mathcal{N}$, compute C_i' as follows:

$$\begin{cases} \text{If } i \in I \wedge \underline{i} = i \wedge i \in S\text{:} & C_i' = \hat{e}(C_i, D_i) = \hat{e}(g^{t_i s}, g^{\frac{r_i}{t_i}}) = \hat{e}(g,g)^{r_i \cdot s} \\ \text{If } i \in I \wedge \underline{i} = \neg i \wedge i \notin S\text{:} & C_i' = \hat{e}(C_i, D_i) = \hat{e}(g^{t_{n+i} s}, g^{\frac{r_i}{t_{n+i}}}) = \hat{e}(g,g)^{r_i \cdot s} \\ \text{If } i \notin I\text{:} & C_i' = \hat{e}(C_i, F_i) = \hat{e}(g^{t_{2n+i} s}, g^{\frac{r_i}{t_{2n+i}}}) = \hat{e}(g,g)^{r_i \cdot s} \end{cases}$$

2. Output a plaintext

$$\frac{\widetilde{C}}{\hat{e}\left(\widehat{C}, \widehat{D}\right) \cdot \prod_{i=1}^n C_i'} = \frac{M \cdot \hat{e}\,(g,g)^{t_0 \cdot s}}{\hat{e}\,(g^s, g^{t_0 - r}) \cdot \hat{e}\,(g,g)^{r \cdot s}} = M.$$

4.2 BB-IBE Scheme

We show BB-IBE [8] construction as follows:

$SetUp_I(1^\kappa)$ Let $\mathbb{G}, \mathbb{G}_T$ be a bilinear group of prime order p, and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map.Given a security parameter 1^κ as input, select a random generator $g \in \mathbb{G}$ and $h, g_2 \in_R \mathbb{G}$. Pick $\alpha \in_R \mathbb{Z}_p^*$ and set $g_1 = g^\alpha$,$MK_I = \alpha$ and set $\pi = \langle g, g_1, g_2, h \rangle$.
Let MK_I be a master secret key, and π be the public parameters.

$KeyGen_I(MK_I, \pi, ID)$ Given master secret key $MK_I = \alpha$, public parameters π and an identity ID as input, the PKG picks $u \in_R \mathbb{Z}_p^*$ and output an IBE secret key as $SK_I = \langle sk_1^I, sk_2^I \rangle = \langle g_2^\alpha \left(g_1^{ID} h\right)^u, g^u \rangle$.

$Encrypt_I(ID, \pi, M)$ Given an identity ID, public parameter π and plaintext $M \in \mathbb{G}_T$ as input, select $w \in_R \mathbb{Z}_p^*$ and output an IBE ciphertext C_I.

$$C_I = \langle C_1, C_2, C_3 \rangle = \left\langle g^w, \left(g_1^{ID} h\right)^w, M\hat{e}(g_1, g_2)^w \right\rangle.$$

$Decrypt_I(SK_I, \pi, C_I)$ Given an IBE secret key SK_I, public parameters π and an IBE ciphertext C_I as input, output a plaintext M.

$$M = \frac{C_3 \hat{e}(sk_2^I, C_2)}{\hat{e}(sk_1^I, C_1)}.$$

4.3 [ABE-IBE] Type Proxy Re-encryption

$KenGen_{A \to I}(S, ID, SK_A, \pi, sk_2^I)$ Given the attribute set S, a delegatee's IBE identity ID, a delegator's ABE secret key SK_A, IBE public parameter π and an IBE user's 2nd component of secret key[1] sk_2^I as input, output a re-encryption key $RK_{A \to I} = \left\langle \widehat{R}_a, \widehat{R}_b, \widehat{R}_c, \widehat{R}_d, \ \{\langle R_i, Q_i \rangle \,|i \in \mathcal{N}\} \right\rangle$ as follows:

1. Set $\widehat{R}_a = \widehat{D} \cdot sk_2^I = g^{t_0 - r} g^u$.
2. Select $\tau \in_R \mathbb{Z}_p$ and set $\widehat{R}_b = \left(g_1^{ID} h\right)^\tau$, $\widehat{R}_c = g^\tau$, $\widehat{R}_d = \hat{e}\,(g_1, g_2)^\tau$.
3. Select $\delta_i \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$, set R_i as follows:

$$\begin{cases} \text{If } i \in S: & R_i = \langle r_{i,1}, r_{i,2} \rangle = \left\langle D_i \cdot g^{\delta_i}, T_i^{\delta_i} \right\rangle \\ \text{If } i \notin S: & R_i = \langle r_{i,1}, r_{i,2} \rangle = \left\langle D_i \cdot g^{\delta_i}, T_{n+i}^{\delta_i} \right\rangle \end{cases}$$

4. For every $i \in \mathcal{N}$, set Q_i as follows:

$$Q_i = \langle q_{i,1}, q_{i,2} \rangle = \left\langle F_i \cdot g^{\delta_i}, T_{2n+i}^{\delta_i} \right\rangle.$$

$ReEncrypt_{A \to I}(RK_{A \to I}, C_A)$ Given a re-encryption key $RK_{A \to I}$ and an ABE ciphertext $C_A = \left\langle W, \widetilde{C}, \widehat{C}, \{C_i | i \in \mathcal{N}\} \right\rangle$ as input, output an IBE ciphertext C_I as follows:

[1] In our [ABE-IBE] type proxy re-encryption scheme, an IBE user must pass own second component of secret key sk_2^I to the ABE user, however this property does not affect security of [8]. This property proved in Lemma 1 of [20].

1. For each $i \in \mathcal{N}$ compute $\overline{C}_i$ as follows:

$$\begin{cases} \text{If } i \in I \wedge \underline{i} = i \wedge i \in S\text{:} & \overline{C}_i = \frac{\hat{e}(C_i, r_{i,1})}{\hat{e}\left(r_{i,2}, \widehat{C}\right)} = \hat{e}(g,g)^{r_i \cdot s} \\ \text{If } i \in I \wedge \underline{i} = \neg i \wedge i \notin S\text{:} & \overline{C}_i = \frac{\hat{e}(C_i, r_{i,1})}{\hat{e}\left(r_{i,2}, \widehat{C}\right)} = \hat{e}(g,g)^{r_i \cdot s} \\ \text{If } i \notin I\text{:} & \overline{C}_i = \frac{\hat{e}(C_i, q_{i,1})}{\hat{e}\left(q_{i,2}, \widehat{C}\right)} = \hat{e}(g,g)^{r_i \cdot s} \end{cases}$$

2. Select $y \in_R \mathbb{Z}_p$ and output $C_I = \langle C_1, C_2, C_3 \rangle$ as follows:

$$\langle C_1, C_2, C_3 \rangle = \left\langle \left(\widehat{R}_c\right)^y, \left(\widehat{R}_b\right)^y \widehat{C}, \frac{\widetilde{C} \cdot \left(\widehat{R}_d\right)^y}{\hat{e}\left(\widehat{C}, \widehat{R}_a\right) \cdot \left(\prod_{i=1}^{n} \overline{C}_i\right)} \right\rangle.$$

Note that, the delegatee can decrypt this re-encrypted result C_I using his own secret key SK_I with same IBE decryption algorithm as follows:

$$\begin{aligned} \frac{C_3 \hat{e}(sk_2^I, C_2)}{\hat{e}(sk_1^I, C_1)} &= \frac{\widetilde{C} \cdot \left(\widehat{R}_d\right)^y \hat{e}\left(sk_2^I, \left(\widehat{R}_b\right)^y \widehat{C}\right)}{\hat{e}\left(\widehat{C}, \widehat{R}_a\right) \cdot \prod_{i=1}^{n} \overline{C}_i \cdot \hat{e}\left(sk_1^I, \left(\widehat{R}_c\right)^y\right)} \\ &= \frac{M \cdot \left(e(g,g)^{t_0}\right)^s \hat{e}(g_1, g_2)^{y\tau} \hat{e}\left(g^u, \left(g_1^{ID} h\right)^{y\tau} g^s\right)}{\hat{e}\left(g^s, g^{t_0 - r} g^u\right) \cdot \prod_{i=1}^{n} \hat{e}(g,g)^{r_i \cdot s} \cdot \hat{e}\left(g_2^{\alpha} \left(g_1^{ID} h\right)^u, g^{y\tau}\right)} = M \end{aligned}$$

5 Security

We next show that ABE-PRE is IND-sAttr-CPA, if the Decisional BDH problem holds in $\mathbb{G}, \mathbb{G}_T$.

Theorem 1. *Suppose that the $(\kappa, t, \epsilon) - DBDH$ assumption holds in $(\mathbb{G}, \mathbb{G}_T)$. Then, the ABE-PRE is $(\kappa, t', q, \epsilon)$-IND-sAttr-CPA secure against an adversary for any (q, κ, ϵ) and $t' < t - \Theta(\tau q)$, where τ denotes a maximum time for exponentiation in $\mathbb{G}, \mathbb{G}_T$.*

Proof. Let $\mathcal{A}$ be a (t, q, ϵ) adversary against the [ABE-IBE] type proxy re-encryption scheme(ABE-IBE-PRE). We construct an adversary $\mathcal{B}$ which can solve the DBDH problem in $\mathbb{G}$ by using $\mathcal{A}$. The $\mathcal{B}$ is given an input $\langle g, \Gamma_a, \Gamma_b, \Gamma_c, \Gamma_T \rangle = \langle g, g^a, g^b, g^c, \Gamma_T \rangle$, and distinguishes Γ_T is $\hat{e}(g,g)^{abc}$ or $\Gamma_T \in_R \mathbb{G}_T$. $\mathcal{B}$ works as follows:

Init $\mathcal{A}$ chooses the following and sends it to $\mathcal{B}$.
- The challenge access structure $W = \bigwedge_{i \in I} \underline{i}$
- The challenge IBE identity ID^*

Setup $\mathcal{B}$ setup simulation as follows:

List SetUp $\mathcal{B}$ generates three blank lists to store a query and answer pairs for every queries, and setup ABE, IBE as follows:

Table 1. ABE Public Key in CPA simulation

	$i \in I$		$i \notin I$
	$\underline{i} = i$	$\underline{i} = \neg i$	
T_i	g^{α_i}	$\Gamma_b^{\alpha_i}$	$\Gamma_b^{\alpha_i}$
T_{n+i}	$\Gamma_b^{\beta_i}$	g^{β_i}	$\Gamma_b^{\beta_i}$
T_{2n+i}	$\Gamma_b^{\gamma_i}$	$\Gamma_b^{\gamma_i}$	g^{γ_i}

$ISKL$ (IBE Secret Key List): Record the tuple $\langle ID, SK_I \rangle$, where ID is an identity of IBE user, SK_I are IBE secret key corresponding to ID.

$ASKL$ (ABE Secret Key List): Record the tuple $\langle S,\ SK_A \rangle$, where S is a set of attributes and SK_A are ABE secret key corresponding to set S.

$REKL$ (Re-Encryption Key List for IBE): Record the tuple $\langle S,\ ID,\ RK_{A \to I} \rangle$, where S is a set of attributes, ID is an identity of IBE user, $RK_{A \to I}$ is a re-encryption key.

ABE SetUp $\mathcal{B}$ sets $T_0 = \hat{e}(\Gamma_a, \Gamma_b) = \hat{e}(g,g)^{ab}$ and chooses $\alpha_i, \beta_i, \gamma_i \in_R \mathbb{Z}_p$ for each $i \in \mathcal{N}$. Then set ABE public key components T_i, T_{n+i} and T_{2n+i} as Table 1.

Under this condition, the first component of ABE master secret key is ab which $\mathcal{B}$ cannot compute.

IBE SetUp Then $\mathcal{B}$ generates random numbers $z_1, z_2, z_3 \in_R \mathbb{Z}_p^*$ and sets $g_1 = \Gamma_a^{z_1}$, $g_2 = \Gamma_b^{z_2}$, $h = g_1^{-ID^*} g^{z_3}$. $\mathcal{B}$ provides public parameters $\pi = \langle g, g_1, g_2, h \rangle$ to $\mathcal{A}$. Under this condition, the master secret key is $MK_I = az_1$ which $\mathcal{B}$ cannot compute.

Phase 1 $\mathcal{A}$ adaptively queries $\mathcal{B}$, and $\mathcal{B}$ responds as follows:

$Extract_A(S)$ $\mathcal{A}$ queries the ABE secret key SK_A, $\mathcal{B}$ as follows:

$\mathcal{A}$ queries the ABE secret key SK_A with a set $S \subseteq \mathcal{N}$ where $S \not\models W$. There must exist $j \in I$ such that, either $j \in S \wedge \underline{j} = \neg j$ or $j \notin S \wedge \underline{j} = j$. $\mathcal{B}$ chooses such j. Without loss of generality, we can assume that $j \notin S \wedge \underline{j} = j$.

For every $i \in \mathcal{N}$, $\mathcal{B}$ chooses $r_i' \in_R \mathbb{Z}_p$. Then sets $r_j = ab + r_j' b$ and for every $i \neq j, i \in \mathcal{N}$,$r_i = r_i' b$. Finally $\mathcal{B}$ sets $r = \sum_{i=1}^n r_i = ab + \sum_{i=1}^n r_i' b$. The $\widehat{D}$ component of the secret key can be computed as

$$\prod_{i=1}^n \frac{1}{\Gamma_b^{r_i'}} = g^{-\sum_{i=1}^n r_i' b} = g^{ab-r}.$$

Recall that $j \in I \setminus S \wedge \underline{j} = j$, then $D_j = \Gamma_a^{\frac{1}{\beta_j}} g^{\frac{r_j'}{\beta_j}} = g^{\frac{ab + r_j' b}{b\beta_j}} = g^{\frac{r_j}{b\beta_j}}$.

For each $i \in I \wedge i \neq j$, ABE secret key components D_i can be computed as follows:

$$\begin{cases} \text{If } i \in S \wedge i \in I \wedge \underline{i} = i\text{:} & D_i = \Gamma_b^{\frac{r_i'}{\alpha_i}} = g^{\frac{r_i}{\alpha_i}}. \\ \text{If } i \in S \wedge ((i \in I \wedge \underline{i} = \neg i) \vee i \notin I)\text{:} & D_i = g^{\frac{r_i'}{\alpha_i}} = g^{\frac{r_i}{b\alpha_i}}. \\ \text{If } i \notin S \wedge ((i \in I \wedge \underline{i} = i) \vee i \notin I)\text{:} & D_i = g^{\frac{r_i'}{\beta_i}} = g^{\frac{r_i}{b\beta_i}}. \\ \text{If } i \notin S \wedge i \in I \wedge \underline{i} = \neg i\text{:} & D_i = \Gamma_b^{\frac{r_i'}{\beta_i}} = g^{\frac{r_i}{\beta_i}}. \end{cases}$$

The ABE secret key components F_i (for *don't care* attribute) can be computed as follows:

1. If $i = j$

$$F_j = \Gamma_a^{\frac{1}{\gamma_j}} g^{\frac{r'_j}{\gamma_j}} = g^{\frac{ab+r'_j b}{b\gamma_j}} = g^{\frac{r_j}{b\gamma_j}}.$$

2. Otherwise $(i \neq j)$

$$\begin{cases} \text{If } i \in I\text{:} & F_i = g^{\frac{r'_i}{\gamma_i}} = g^{\frac{r_i}{b\gamma_i}} \\ \text{If } i \notin I\text{:} & F_i = \Gamma_b^{\frac{r'_i}{\gamma_i}} = g^{\frac{r_i}{\gamma_i}} \end{cases}$$

$\mathcal{B}$ answers SK_A and writes down to the $ASKL$.

$Extract_I(ID)$ $\mathcal{A}$ queries the IBE user's secret key SK_I with an identity ID.

1. If the $ID = ID^*$, $\mathcal{B}$ rejects.
2. If the $ID \neq ID^*$,$\mathcal{B}$ checks the $REKL$, and if already answers re-encryption key to the ID and $S \models W$, $\mathcal{B}$ rejects.
3. Otherwise $\mathcal{B}$ answers $SK_I = \langle sk_1^I, sk_2^I \rangle$ as follows. $\mathcal{B}_I$ generates a random number $u \in_R \mathbb{Z}_p^*$ and computes $SK_I = \langle sk_1^I, sk_2^I \rangle$ as follows:

$$sk_1^I = \Gamma_b^{\frac{-z_2 z_3}{(ID-ID^*)}} \left(\Gamma_a^{z_1(ID-ID^*)} g^{z_3} \right)^u, sk_2^I = \Gamma_b^{\frac{-z_2}{(ID-ID^*)}} g^u$$

$\mathcal{B}$ answers SK_I and writes down to the $ISKL$.

$Extract_{A \to I}(S, ID)$ $\mathcal{A}$ queries the re-encryption key which can transform ABE ciphertext corresponding to the set S, $\mathcal{B}$ answers a re-encrypt key $RK_{A \to I} = \left\langle \widehat{R}_a, \widehat{R}_b, \widehat{R}_c, \widehat{R}_d, \{\langle R_i, Q_i \rangle \,|i \in \mathcal{N}\} \right\rangle$ as follows:

1. If $S \not\models W$,
   $\mathcal{B}$ runs $Extract_A(S)$ and obtain an ABE secret key $SK_A = \left\langle \widehat{D}, \{\langle D_i, F_i \rangle \,|i \in \mathcal{N}\} \right\rangle$, then chooses $\tau, u \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$.
   (a) If $ID \neq ID^*$, $\mathcal{B}$ sets re-encryption key components $\widehat{R}_a$, $\widehat{R}_b$, $\widehat{R}_c$, $\widehat{R}_d$ as follows:

$$\widehat{R}_a = \widehat{D} \Gamma_b^{\frac{-z_2}{ID-ID^*}} g^u, \widehat{R}_b = \left(\Gamma_a^{z_1(ID-ID^*)} g^{z_3} \right)^\tau,$$
$$\widehat{R}_c = g^\tau, \widehat{R}_d = \hat{e}\left(\Gamma_a^{z_1}, \Gamma_b^{z_2}\right)^\tau$$

   Note that, let $u' = \frac{-bz_2}{ID-ID^*}$, simulated $\widehat{R}_a$ and $\widehat{R}_b$ can be transform as follows:

$$\widehat{R}_a = \widehat{D} \Gamma_b^{\frac{-z_2}{ID-ID^*}} g^u = g^{u'},$$
$$\widehat{R}_b = \left(\Gamma_a^{z_1(ID-ID^*)} g^{z_3} \right)^\tau = \left(\Gamma_a^{z_1 ID} h \right)^\tau = \left(g_1^{ID} h \right)^\tau$$

   (b) If $ID = ID^*$, $\mathcal{B}$ sets re-encryption key components $\widehat{R}_a$, $\widehat{R}_b$, $\widehat{R}_c$, $\widehat{R}_d$ as follows:

$$\widehat{R}_a = \widehat{D} g^u, \widehat{R}_b = \left(g^{z_3}\right)^\tau, \widehat{R}_c = g^\tau, \widehat{R}_d = \hat{e}\left(\Gamma_a^{z_1}, \Gamma_b^{z_2}\right)^\tau$$

Note that, simulated $\widehat{R}_b$ can be transform as follows:

$$\widehat{R}_b = (g^{z_3})^{\tau} = \left(g_1^{ID^*} g_1^{-ID^*} g^{z_3}\right)^{\tau} = \left(g_1^{ID^*} h\right)^{\tau}$$

After the success of above simulation, $\mathcal{B}$ chooses $\delta_i \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$and $\phi \in_R \mathbb{Z}_p$ and sets re-encryption key components R_i, Q_i as follows:

$$R_i = \begin{cases} i \in S: & \left\langle D_i \cdot g^{\delta_i}, T_i^{\delta_i} \right\rangle \\ i \neq\in S: & \left\langle D_i \cdot g^{\delta_i}, T_{n+i}^{\delta_i} \right\rangle \end{cases}$$
$$Q_i = \left\langle F_i \cdot g^{\delta_i}, T_{2n+i}^{\delta_i} \right\rangle$$

2. Otherwise ($S \models W$),
$\mathcal{B}$ chooses $\rho_i \in_R \mathbb{Z}_p$ for every $i \in \mathbb{N}$ and sets $\rho = \sum_{i=1}^{n} \rho_i \bmod p$. $\mathcal{B}$ chooses $\tau \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$.
   (a) $\mathcal{B}$ checks, and if already answers IBE secret key for ID, $\mathcal{B}$ rejects.
   (b) If $ID \neq ID^*$, $\mathcal{B}$ sets re-encryption key components $\widehat{R}_a$, $\widehat{R}_b$, $\widehat{R}_c$, $\widehat{R}_d$ as follows:

$$\widehat{R}_a = \Gamma_b^{-\rho} \Gamma_b^{\frac{-z_2 u}{ID-ID^*}}, \widehat{R}_b = \left(\Gamma_a^{z_1(ID-ID^*)} g^{z_3}\right)^{\tau},$$
$$\widehat{R}_c = g^{\tau}, \widehat{R}_d = \hat{e}\left(\Gamma_a^{z_1}, \Gamma_b^{z_2}\right)^{\tau}$$

Note that, let $u' = -ab - \frac{buz_2}{ID-ID^*}$ and $r' = b\rho$, simulated $\widehat{R}_a$,$\widehat{R}_b$ can be transform as follows:

$$\widehat{R}_a = \Gamma_b^{-\rho} \Gamma_b^{\frac{-z_2 u}{ID-ID^*}} = g^{ab-b\rho} g^{-ab} g^{\frac{-buz_2}{ID-ID^*}} = g^{ab-r'} g^{u'},$$
$$\widehat{R}_b = \left(\Gamma_a^{z_1(ID-ID^*)} g^{z_3}\right)^{\tau} = \left(\Gamma_a^{z_1 ID} h\right)^{\tau} = \left(g_1^{ID} h\right)^{\tau}$$

Under this condition, $\mathcal{B}$ cannot compute an IBE secret key for ID, however $\mathcal{B}$ can reject the IBE secret key query for the ID.
   (c) If $ID = ID^*$, $\mathcal{B}$ sets re-encryption key components $\widehat{R}_a$, $\widehat{R}_b$, $\widehat{R}_c$, $\widehat{R}_d$ as follows:

$$\widehat{R}_a = g^{-\rho}, \widehat{R}_b = (g^{z_3})^{\tau}, \widehat{R}_c = g^{\tau}, \widehat{R}_d = \hat{e}\left(\Gamma_a^{z_1}, \Gamma_b^{z_2}\right)^{\tau}$$

Note that, let $u' - r = -ab - \rho$, simulated $\widehat{R}_a$ can be transform as follows:

$$\widehat{R}_a = g^{-\rho} = g^{ab-\rho} g^{-ab} = g^{ab-r} g^{u'},$$
$$\widehat{R}_b = (g^{z_3})^{\tau} = \left(g_1^{ID^*} g_1^{-ID^*} g^{z_3}\right)^{\tau} = \left(g_1^{ID^*} h\right)^{\tau}$$

Under this condition, $\mathcal{B}$ cannot compute an IBE secret key for ID^*, however $\mathcal{B}$ can reject the IBE secret key for the ID^*.

After the success of above simulation, $\mathcal{B}$ chooses $\delta_i \in_R \mathbb{Z}_p$ for every $i \in \mathcal{N}$and $\phi \in_R \mathbb{Z}_p$ and sets re-encryption key components R_i, Q_i as follows:

$$R_i = \begin{cases} i \in S: & \left\langle g^{\frac{\rho_i}{\alpha_i}} \cdot g^{\delta_i}, T_i^{\delta_i} \right\rangle \\ i \notin S: & \left\langle g^{\frac{\rho_i}{\beta_i}} \cdot g^{\delta_i}, T_{n+i}^{\delta_i} \right\rangle \end{cases}$$

$$Q_i = \left\langle g^{\frac{\rho_i}{\gamma_i}} \cdot g^{\delta_i}, T_{2n+i}^{\delta_i} \right\rangle$$

Challenge. $\mathcal{A}$ submits two equal length plaintexts $M_0, M_1 \in \mathbb{G}_T$ and selects which scheme to attack. $\mathcal{B}$ chooses $\mu \in \{0,1\}$ and outputs a challenge ciphertext as follows:

- If $\mathcal{A}$ selects ABE scheme to attack, $\mathcal{B}$ outputs an ABE ciphertext for a challenge access structure $C_A^* = \left\langle \widetilde{C}^*, \widehat{C}^*, \{C_i^* | i \in I\} \right\rangle$ as follows:

$$\widetilde{C}^* = M_\mu \Gamma_T, \widehat{C}^* = \Gamma_c,$$
$$C_i^* = \left\{ \{\Gamma_c^{\alpha_i} | i \in I \wedge \underline{i} = i\}, \{\Gamma_c^{\beta_i} | i \in I \wedge \underline{i} = \neg i\}, \{\Gamma_c^{\gamma_i} | i \notin I\} \right\}$$

- If $\mathcal{A}$ selects IBE scheme to attack, $\mathcal{B}$ outputs a IBE ciphertext $C_I^* = \langle C_1, C_2, C_3 \rangle$ corresponding to a target identity ID^* as follows:

$$C_1 = \Gamma_c, C_2 = (\Gamma_c)^{z_3}, C_3 = M_\mu (\Gamma_T)^{z_1 z_2}$$

Phase 2. $\mathcal{B}$ answers $\mathcal{A}$'s queries in same manner of Phase 1.

Solve. Finally, $\mathcal{A}$ outputs a guess result $\mu' \in \{0,1\}$. If $\mu' = \mu$, then $\mathcal{B}$ judges $\Gamma_T = \hat{e}(g,g)^{abc}$ and outputs 1. Otherwise, $\mathcal{B}$ judges $\Gamma_T \in_R \mathbb{G}_T$ and outputs 0.

We claim that in the above simulation answers of $\mathcal{B}$ are correctly distributed, and $\mathcal{A}$ cannot distinguish our simulation from the real-world interaction. Furthermore, $Adv_{\mathcal{A}}^{DBDH} = Adv_{\mathcal{A}}^{\mathcal{S}}$, because $\mathcal{B}$ does not abort during the above simulation.

In the above simulation, maximum computation cost of the queries is at most polynomial time exponentiation, hence $t' < t - \Theta(\tau q)$. Therefore, the ABE-IBE-PRE is $(\kappa, t', q, \epsilon)$-IND-sAttr-CPA secure against an adversary.

6 Extension

In our scheme, the delegator can delegate a part of his decryption rights. The delegator can pass subset of the ABE secret key SK'_A and subset of S' to generate a re-encryption key for substitute of SK_A. The subset of the ABE secret key SK'_A at least have a *positive* or *negative* or *don't care* component for each attribute. On the other hand, the full set of the ABE secret key SK_A have a *positive* or *negative* component and *don't care* component for each attribute.

For example, if the delegator passes *positive* component and does not passes *don't care* component for some attribute, then the proxy cannot convert ciphertexts which have *don't care* policy for the attribute.

7 Conclusion

In this paper, we propose new proxy re-encryption scheme which can convert an ABE ciphertext to an IBE ciphertext. Our scheme achieves proxy invisible which means delegatee does not aware of existence of the proxy. We define the security notation and prove security based on DBDH assumption in the standard model against chosen plaintext attack. To achieve the CCA security and adaptive-ID security is further study. However, it should be possible to change [8] to [4] to achieve adaptive ID security.

Furthermore, [ABE-PKE] type proxy, and conbination of types such as [IBE-ABE] and [PKE-ABE], [ABE-ABE] might be useful, but it is also further study.

Acknowledgement

We thank the anonymous reviewers for many useful comments.

References

1. Joux, A.: A one round protocol for tripartite diffie-hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–394. Springer, Heidelberg (2000)
2. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
3. Libert, B., Vergnaud, D.: Unidirectional chosen-ciphertext secure proxy re-encryption. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 360–379. Springer, Heidelberg (2008)
4. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
5. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Cryptology ePrint Archive, Report 2008/290 (2008), `http://eprint.iacr.org/2008/290.pdf`
6. Chu, C., Tzeng, W.: Identity-based proxy re-encryption without random oracles. In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) ISC 2007. LNCS, vol. 4779, pp. 189–202. Springer, Heidelberg (2007)
7. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
8. Boneh, D., Boyen, X.: Efficient selectiveid secure identity based encryption without random oracle. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
9. Ateniese, G., Benson, K., Hohenberger, S.: Key-private proxy re-encryption. In: Cryptology ePrint Archive, Report 2008/463 (2008), `http://eprint.iacr.org/2008/463.pdf`
10. Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage. In: Proceedings of the 12th Annual Network and Distributed System Security Symposium - NDSS 2005, pp. 83–107 (2005)

11. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proc. IEEE Symposium on Security and Privacy, pp. 321–334. IEEE, Los Alamitos (2007)
12. Cheung, L., Newport, C.: Provably secure ciphertext policy abe. In: CCS 2007, pp. 456–465 (2007)
13. Zbou, L., Marsh, M.A., Schneider, F.B., Redz, A.: Distributed blinding for elgamal reencryption. Technical Report 2004-1924. Cornell Computer Science Department (2004)
14. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998)
15. Green, M., Ateniese, G.: Indentity-based proxy re-encryption. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 288–306. Springer, Heidelberg (2007)
16. Jakobsson, M.: On quorum controlled asymmetric proxy re-encryption. In: Imai, H., Zheng, Y. (eds.) PKC 1999. LNCS, vol. 1560, pp. 112–121. Springer, Heidelberg (1999)
17. Mambo, M., Okamoto, E.: Proxy cryptosystems: @delegation of the power to decrypt ciphertexts. IEICE Trans. Fund. Electronics Communications and Computer Science, IEICE E80-A/1, 54–63 (1997)
18. Canetti, R., Hohenberger, S.: Chosen-ciphertext secure proxy re-encryption. In: CCS 2007, pp. 185–194. ACM, New York (2007)
19. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairings. In: Proceedings of the Symposium on Cryptography and Information Security, SCIS 2000 (2000)
20. Matsuo, T.: Proxy re-encryption systems for identity-based encryption. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 247–267. Springer, Heidelberg (2007)
21. Mizuno, T., Doi, H.: Efficient ibe-pke proxy re-encryption. In: International Conference on Security and Cryptography (SECRYPT 2008), pp. 285–293. Insticc Press (2008)
22. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: CCS 2006, pp. 89–98 (2006)
23. Dodis, Y., Ivan, A.: Proxy cryptography revisited. In: Proceedings of the 10th Annual Network and Distributed System Security Symposium- NDSS 2003 (2003)