On the Insecurity of Proxy Re-encryption from IBE to IBE in P1363.3/D1

Xu an Wang

Key Laboratory of Information and Network Security
Engneering College of Chinese Armed Police Force, P.R. China
wangxahq@yahoo.com.cn

Abstract. In 1998, Blaze, Bleumer and Strauss proposed a kind of cryptographic primitive called proxy re-encryption[2]. In proxy re-encryption, a proxy can transform a ciphertext computed under Alice's public key into one that can be opened under Bob's decryption key. In 2007, Matsuo proposed two types of re-encryption schemes which can re-encrypt the ciphertext from CBE to IBE and IBE to IBE [16]. Now these schemes are being standardized by IEEEP1363.3 working group[15]. In this paper, we show that their proxy re-encryption scheme from IBE to IBE is not secure. Specially, in their scheme the proxy himself only can re-encrypt any IBE user's ciphertext into being the delegatee's ciphertext. Thus, the proxy is too powerful in their scheme. We also propose a new secure scheme and prove its security.

1 Introduction

The concept of proxy re-cryptography comes from the work of Blaze, Bleumer, and Strauss in 1998. The goal of proxy re-encryptiohn is to securely enable the re-encryption of ciphertexts from one key to another, without relying on trusted parties.In 2005, Ateniese et al proposed a few new re-encryption schemes and discussed its several potential applications. Since then, many excellent schemes have been proposed,including re-encryption schemes in certificate based setting[7, 13, 12, 14],re-encryption schemes in identity based setting [11, 16, 8, 17]and re-encryption schemes in hybrid setting[16]. Now the IEEE P1363.3 standard working group is setting up a standard with pairing including re-encryption[15].

In 2007, Matsuo proposed two types of re-encryption scheme which can re-encrypt the ciphertext from CBE to IBE and IBE to IBE [16]. Now these two schemes are being standardized by IEEEP1363.3 working group[15]. In this paper, we show that their proxy re-encryption scheme from IBE to IBE is not secure. Specially, in their scheme the proxy himself can re-encrypt any IBE user's ciphertext into a predefined delegatee's ciphertext. Thus, the proxy is two powerful in their scheme, We also propose a rescue scheme based on their scheme.

We organize our paper as following. In section 2, we revisit the proxy re-encryption from IBE to IBE proposed in [16]. In section 3, we give an attack to their scheme. In section 4 ,we give a new scheme which can resist this attack.

In section 5, we discuss the reasons why their scheme is not secure. We give our conclusion in section 6.

2 Revisit the Proxy Re-encryption Scheme from IBE to IBE

The proxy re-encryption scheme from IBE to IBE is based on the BB1-IBE scheme.

- The underlying IBE scheme (BB1-IBE scheme):
  1. $\mathbf{SetUp_{IBE}(k)}$.Given a security parameter k, select a random generator $g \in G$ and random elements $g_2, h \in G$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$,$mk = g_2^\alpha$, and $parms = (g, g_1, g_2, h)$. Let mk be the master-secret key and let $parms$ be the public parameters.
  2. $\mathbf{KeyGen_{IBE}(mk, parms, ID)}$. Given $mk = g_2^\alpha$ and ID with $parms$, pick a random $u \in Z_p^*$. Set $sk_{ID} = (d_0, d_1) = (g_2^\alpha (g_1^{ID} h)^u, g^u)$.
  3. $\mathbf{Enc_{IBE}(ID, parms, M)}$. To encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $C_{ID} = (g^r, (g_1^{ID} h)^r, Me(g_1, g_2)^r) \in G^2 \times G_1$.
  4. $\mathbf{Dec_{IBE}(sk_{ID}, parms, C_{ID})}$. Given ciphertext $C_{ID} = (C_1, C_2, C_3)$ and the secret key $sk_{ID} = (d_0, d_1)$ with $prams$, compute $M = C_3 e(d_1, C_2)/e(d_0, C_1)$.
- The delegation scheme:
  1. $\mathbf{EGen(sk_{ID}, parms)}$. Given $sk_{ID} = (d_0, d_1) = (g_2^\alpha (g_1^{ID} h)^u, g^u)$ for ID with $parms$, set $e_{ID} = d_1 = g^u$.
  2. $\mathbf{KeyGen_{PKG}(mk, parms)}$. Given $mk = \alpha$ with $parms$, set $sk_R = \alpha$.
  3. $\mathbf{KeyGen_{PRO}(sk_R, e_{ID'}, parms, ID, ID')}$. Given $sk_R = \alpha, e_{ID'} = g^{u'}$ with $parms$, set $rk_{ID \to ID'} = (ID \to ID', g^{u' \alpha})$.
  4. $\mathbf{ReEnc(rk_{ID \to ID'}, parms, C_{ID}, ID')}$. Given the delegator's identity ID, the delegatee's identity ID', $rk_{ID \to ID'} = (ID \to ID', g^{u' \alpha})$,$C_{ID} = (C_1, C_2, C_3)$ with $parms$, re-encrypt the ciphertext C_{ID} into $C_{ID'}$ as follows.First it runs "Check", if output 0, then return "Reject". Else computes $C_{ID'} = (C_1', C_2', C_3') = (C_1, C_2, C_3 e(C_1^{ID' - ID}, g^{u' \alpha})) \in G^2 \times G_1$.
  5. $\mathbf{Check(parms, C_{ID}, ID)}$. Given the delegator's identity ID and $C_{ID} = (C_1, C_2, C_3)$ with $parms$, compute $v_0 = e(C_1, g_1^{ID} h)$ and $v_1 = (C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.

We can verify the correctness of the re-encrypted ciphertext as following,

$$\begin{aligned}
\frac{C_3' e(d_1, C_2')}{e(d_0, C_1')} &= \frac{M \cdot e(g_1, g_2)^r e(g^{r(ID' - ID)}, g^{u' \alpha}) e(g^{u'}, (g_1^{ID} h)^r)}{e(g_2^\alpha (g_1^{ID'} h)^{u'}, g^r)} \\
&= \frac{M \cdot e(g_1, g_2)^r e({g_1}^{r(ID' - ID)}, g^{u'}) e(g^{u'}, (g_1^{ID} h)^r)}{e(g_2^\alpha (g_1^{ID'} h)^{u'}, g^r)} \\
&= \frac{M \cdot e(g_1, g_2)^r e((g_1^{ID} h)^r \cdot g_1^{r(ID' - ID)}, g^{u'})}{e(g_2^\alpha (g_1^{ID'} h)^{u'}, g^r)}
\end{aligned}$$

$$\begin{aligned}
&= \frac{M \cdot e(g_1, g_2)^r e((g_1^{ID'} h)^r, g^{u'})}{e(g_2^{\alpha}(g_1^{ID'} h)^{u'}, g^r)} \\
&= \frac{M \cdot e(g_1, g_2)^r e((g_1^{ID'} h)^r, g^{u'})}{e(g_1, g_2)^r e((g_1^{ID'} h)^r, g^{u'})} \\
&= M
\end{aligned}$$

Now this scheme is being standardized by IEEEP1363.3 working group[15].

3 An Attack to the Proxy Re-encryption Scheme from IBE to IBE in P1363.3/D1

We note that in the scheme the re-encryption is $rk_{ID \to ID'} = (ID \to ID', g^{u'\alpha})$. In this key we can not see any secret value contributed by the delegator, thus the proxy can re-encrypt any ID's ciphertext into ID''s ciphertext. Suppose there is another IBE user ID'' with a ciphertext $C_{ID''} = (C_1'', C_2'', C_3'') = (g^{r'}, (g_1^{ID''} h)^{r'}, Me(g_1, g_2)^{r'})$ which has not been agreed about the delegation with ID', but the proxy can re-encrypt ID'''s ciphertext into ID''s valid ciphertext. Thus ID' can decrypt ID'''s ciphertext, which is not secure at all. Following is the attack.

1. First the proxy runs "Check". Because $C_{ID''} = (C_1'', C_2'', C_3'')$ is a valid ciphertext for ID'', thus the proxy can go through.
2. Second the proxy runs "ReEnc" . Given the delegator's identity ID'', the delegatee's identity ID', $rk_{ID'' \to ID'} = (ID'' \to ID', g^{u'\alpha})$,$C_{ID''} = (C_1'', C_2'', C_3'')$ with *parms*, re-encrypt the ciphertext $C_{ID''}$ into $C_{ID'}$ as follows. $C_{ID'} = (C_1', C_2', C_3') = (C_1'', C_2'', C_3'' e(C_1''^{ID''-ID}, g^{u'\alpha})) \in G^2 \times G_1$. And this ciphertext is a valid ciphertext for ID' as following

$$\begin{aligned}
\frac{C_3' e(d_1, C_2')}{e(d_0, C_1')} &= \frac{M' \cdot e(g_1, g_2)^{r'} e(g^{r'(ID''-ID)}, g^{u'\alpha}) e(g^{u'}, (g_1^{ID''} h)^{r'})}{e(g_2^{\alpha}(g_1^{ID'} h)^{u'}, g^{r'})} \\
&= \frac{M' \cdot e(g_1, g_2)^{r'} e({g_1}^{r'(ID'-ID'')}, g^{u'}) e(g^{u'}, (g_1^{ID''} h)^{r'})}{e(g_2^{\alpha}(g_1^{ID'} h)^{u'}, g^{r'})} \\
&= \frac{M' \cdot e(g_1, g_2)^{r'} e((g_1^{ID''} h)^{r'} \cdot g_1^{r'(ID'-ID'')}, g^{u'})}{e(g_2^{\alpha}(g_1^{ID'} h)^{u'}, g^{r'})} \\
&= \frac{M' \cdot e(g_1, g_2)^{r'} e((g_1^{ID'} h)^{r'}, g^{u'})}{e(g_2^{\alpha}(g_1^{ID'} h)^{u'}, g^{r'})} \\
&= \frac{M' \cdot e(g_1, g_2)^{r'} e((g_1^{ID'} h)^{r'}, g^{u'})}{e(g_1, g_2)^{r'} e((g_1^{ID'} h)^{r'}, g^{u'})} \\
&= M'
\end{aligned}$$

Thus ID' can decrypt every ID'''s ciphertext if it colludes with the proxy.

4 A New Scheme and Its Security Proof

4.1 Our Proposed Scheme

- The underlying IBE scheme:

  1. **SetUp$_{\mathbf{IBE}}$(k)**.Given a security parameter k, select a random generator $g \in G$, choose randomly $t_1, t_2 \in Z_p^*$ and computes elements $g_2 = g^{t_1}, h = g^{t_2} \in G$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^{\alpha}$,$mk = (g_2^{\alpha}, t_1, t_2)$, and $parms = (g, g_1, g_2, h)$. Let mk be the master- secret key and let $parms$ be the public parameters.
  2. **KeyGen$_{\mathbf{IBE}}$(mk, parms, ID)**. Given $mk = g_2^{\alpha}$ and ID with $parms$, pick a random $u \in Z_p^*$. Set $sk_{ID} = (d_0, d_1) = (g_2^{\alpha}(g_1^{ID}h)^u, g^u)$. The KGC preserves a `user-key-list` of form (ID, u) and makes it be secret.
  3. **Enc$_{\mathbf{IBE}}$(ID, parms, M)**. To encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, pick a random $r \in Z_p^*$ and compute $C_{ID} = (g^r, (g_1^{ID}h)^r, Me(g_1, g_2)^r) \in G^2 \times G_1$.
  4. **Dec$_{\mathbf{IBE}}$(sk$_{\mathbf{ID}}$, parms, C$_{\mathbf{ID}}$)**. Given ciphertext $C_{ID} = (C_1, C_2, C_3)$ and the secret key $sk_{ID} = (d_0, d_1)$ with $prams$, compute $M = C_3e(d_1, C_2)/e(d_0, C_1)$.

- The delegation scheme:

  1. **KeyGen$_{\mathbf{PRO}}$(sk$_{\mathbf{R}}$, parms, ID, ID$'$)**. The KGC searches in the `user-key-list` for ID', if find no item of (ID', u'), then return "Reject", otherwise it chooses a randomly $k \in Z_p^*$, computes $w = g_1^k$ and makes it be public. The KGC sets $rk_{ID \to ID'} = (ID \to ID', \frac{u'+k}{\alpha ID + t_2})$. We must note that the KGC chooses a different k for every different user pair (ID, ID').
  2. **ReEnc(rk$_{\mathbf{ID} \to \mathbf{ID}'}$, parms, C$_{\mathbf{ID}}$, ID$'$)**. Given the delegator's identity ID, the delegatee's identity ID', $rk_{ID \to ID'} = (ID \to ID', \frac{u'+k}{\alpha ID + t_2})$,$C_{ID} = (C_1, C_2, C_3)$ with $parms$, re-encrypt the ciphertext C_{ID} into $C_{ID'}$ as follows. First it runs "Check", if output 0, then return "Reject". Else computes $C_{ID'} = (C_1', C_2', C_3') = (C_1, C_2, \frac{C_3 e(C_2^{rk_{ID \to ID'}}, g_1^{(ID'-ID)})}{e(w^{(ID'-ID)}, C_1)}) \in G^2 \times G_1$.
  3. **Check(parms, C$_{\mathbf{ID}}$, ID)**. Given the delegator's identity ID and $C_{ID} = (C_1^k, C_2, C_3)$ with $parms$, compute $v_0 = e(C_1, g_1^{ID}h)$ and $v_1 = (C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.

We can verify its correctness as the following

$$\frac{C_3' e(d_1, C_2')}{e(d_0, C_1')} = \frac{M \cdot e(g_1, g_2)^r e(C_2^{rk_{ID \to ID'}}, g_1^{(ID'-ID)}))e(g^{u'}, (g_1^{ID}h)^r)}{e(w^{(ID'-ID)}, C_1)e(g_2^{\alpha}(g_1^{ID'}h)^{u'}, g^r)}$$

$$
\begin{aligned}
&= \frac{M \cdot e(g_1, g_2)^r e((g_1^{ID}h)^{r\frac{u'+k}{\alpha ID+t_2}}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e(g_2^{\alpha}(g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me((g_1^{ID}h)^{r\frac{u'+k}{\alpha ID+t_2}}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me((g^{\alpha ID+t_2})^{r\frac{u'+k}{\alpha ID+t_2}}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^{(u'+k)r}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^{kr}, g_1^{(ID'-ID)}) e(g^{u'r}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^{u'r}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^r, g_1^{u'(ID'-ID)}) e(g^r, (g_1^{ID}h)^{u'})}{e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^r, g_1^{u'ID'}h^{u'})}{e((g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{Me(g^r, (g_1^{ID'}h)^{u'})}{e((g_1^{ID'}h)^{u'}, g^r)} \\
&= M
\end{aligned}
$$

Remark 1. In our scheme, we must note that the KGC chooses a different k for every different user pair (ID, ID'). Otherwise, if the adversary know $\frac{u'+k}{\alpha ID+t_2}$ for three different ID_1, ID_2, ID_3 but one k and ID' , he can compute α, t_2, which is not secure of course. We also note the KGC must let $w = g_1^k$ be public. This can be realized by signature schemes. Assuming the KGC choose private ,public key and signature algorithm(sk, vk, Σ), he let (sk, vk, Σ) be one part of his *params*.The KGC can sign $\Sigma_{sk}(w, ID, ID')$, thus everyone can verify w being authenticated. We also realize that in our scheme the KGC needs publicize every different w for every different (ID, ID'), which is a shortcoming we need to improve in the future.

4.2 Security Proof

First we define the following oracles, which can be invoked multiple times in any order, subject to the constraints list in the various definition:

- **Uncorrupted user's key generation (O_{keygen}):** Obtain a new key pair as $(ID, sk_{ID}) \leftarrow KeyGen_{IBE}(1^k)$. A is given ID .

- **Corrupted user's key generation** **(**$O_{corkeygen}$**):** Obtain $sk_{ID} \leftarrow KeyGen_{IBE}$ $(mk, parms, ID)$. A is given sk_{ID}.
- **Re-encryption key generation** **(**$O_{rekeygen}$**)**:On input (ID_1, ID_2) by the adversary, where ID_1 and ID_2 are two users in IBE setting, return the re-encryption key $ReKeyGen_{PRO}(ID_1, ID_2)$.
- **Encryption oracle**$O_{enc_{IBE}}$**:** For IBE users, to encrypt a message $M \in G_1$ under the public key $ID \in Z_p^*$, return $Enc_{IBE}(ID, parms, M)$.
- **Re-encryption** O_{renc}**:** Output the re-encrypted ciphertext $ReEnc(rk_{ID_1,ID_2},$ $params, C_{ID_1}, ID_2)$.

Internal and External Security. Our security model protects users from two types of attacks: those launched from parties outside the system (External Security), and those launched from parties inside the system, such as the proxy, another delegation partner or some collusion between them (Internal Security). Generally speaking, internal adversaries are more powerful than external adversaries. We give the security models as following.

Delegator Security.

Definition 1. (Delegator-IBE-IND-ID-CPA) *A PRE scheme from IBE to IBE is IBE-IND-ID-CPA secure if the probability*
$Pr[sk_{ID^\star} \leftarrow O_{keygen}(\lambda), \{sk_{ID_x} \leftarrow O_{corkeygen}(\lambda)\}, \{sk_{ID_h} \leftarrow O_{keygen}(\lambda)\},$
$\{R_{hx} \leftarrow O_{rekeygen}(ID_h, sk_{ID_x})\}, \{R_{xh} \leftarrow O_{rekeygen}(ID_x, sk_{ID_h})\},$
$\{R_{\star h} \leftarrow O_{rekeygen(ID^\star, sk_{ID_h})}\}, \{R_{\star x} \leftarrow O_{rekeygen(ID^\star, sk_{ID_x})}\}$
$(m_0, m_1, St) \leftarrow A^{O_{renc}, O_{enc_{IBE}}}(ID^\star, \{sk_{ID_x}\}, \{R_{xh}\}, \{R_{hx}\}, \{R_{\star h}\}, \{R_{\star x}\}),$
$d^\star \xleftarrow{R} \{0,1\}, C^\star = enc_{IBE}(m_{d^\star}, ID^\star), d' \leftarrow A^{O_{renc}, O_{enc_{IBE}}}(C^\star, St) : d' = d^\star]$
is negligibly close to $1/2$ *for any PPT adversary* A*. In the above game, any query to oracle* O_{renc} *which makes the output is* $C_\star$ *is returned with* $\perp$*. In our notation,* St *is a state information maintained by* A *while* $sk^\star$ *is the target user's pubic and private key pair, the challenger also chooses other keys for corrupt and honest parties. For other honest parties, keys are subscripted by* h *or* h' *and we subscript corrupt keys by* x *or* x'*. In the game,* A *is said to have advantage* ϵ *if this probability, taken over random choices of* A *and all oracles, is at least* $1/2 + \epsilon$*.*

Delegatee Security.

Definition 2. (Delegatee-IBE-IND-ID-CPA) *A PRE scheme from IBE to IBE is IBE-IND-ID-CPA secure if the probability*
$Pr[sk_{ID^\star} \leftarrow O_{keygen}(\lambda), \{sk_{ID_x} \leftarrow O_{corkeygen}(\lambda)\}, \{sk_{ID_h} \leftarrow O_{keygen}(\lambda)\},$
$\{R_{hx} \leftarrow O_{rekeygen}(ID_h, sk_{ID_x})\}, \{R_{xh} \leftarrow O_{rekeygen}(ID_x, sk_{ID_h})\},$
$\{R_{h\star} \leftarrow O_{rekeygen(sk_{ID_h}, ID^\star)}\}, \{R_{x\star} \leftarrow O_{rekeygen(sk_{ID_x}, ID^\star)}\}$
$(m_0, m_1, St) \leftarrow A^{O_{renc}, O_{enc_{IBE}}}(ID^\star, \{sk_{ID_x}\}, \{R_{xh}\}, \{R_{hx}\}, \{R_{h\star}\}, \{R_{x\star}\}),$
$d^\star \xleftarrow{R} \{0,1\}, C^\star = enc_{IBE}(m_{d^\star}, ID^\star), d' \leftarrow A^{O_{renc}, O_{enc_{IBE}}}(C^\star, St) : d' = d^\star]$
is negligibly close to $1/2$ *for any PPT adversary* A*. In the above game, any query to oracle* O_{renc} *which makes the output is* $C_\star$ *is returned with* $\perp$*. In our*

notation, St is a state information maintained by A while $sk^\star$ is the target user's pubic and private key pair, the challenger also chooses other keys for corrupt and honest parties. For other honest parties, keys are subscripted by h or h' and we subscript corrupt keys by x or x'. In the game, A is said to have advantage ϵ if this probability, taken over random choices of A and all oracles, is at least $1/2 + \epsilon$.

KGC Security.

In proxy re-encryption from IBE to IBE, KGC's master secret key can not leverage even if the delegator, the delegatee and proxy collude.

Definition 3. (KGC-OW) *A PRE scheme from IBE to IBE is secure for KGC if the probability*
$Pr[\{sk_{ID_x} \leftarrow O_{corkeygen}(\lambda)\}, \{sk_{ID_h} \leftarrow O_{keygen}(\lambda)\},$
$\{R_{xx'} \leftarrow O_{rekeygen(ID_{x'},ID_x)}\}, \{R_{x'x} \leftarrow O_{rekeygen(ID_x,ID'_x)}\},$
$\{R_{hx} \leftarrow O_{rekeygen}(ID_h, ID_x)\}, \{R_{xh} \leftarrow O_{rekeygen}(ID_x, ID_h)\},$
$mk' \leftarrow A^{O_{renc},O_{enc_{IBE}}}(St, \{sk_{ID_x}\}, \{R_{xh}\}, \{R_{hx}\}, \{R_{xx'}\}, \{R_{x'x}\}, \{parms\}) :$
$mk = mk']$

is negligibly close to 0 for any PPT adversary A. In our notation, St is a state information maintained by A, For the honest parties, keys are subscripted by h or h' and we subscript corrupt keys by x or x'.

Theorem 1. *Suppose the DBDH assumption holds, then our scheme is Delegator-IBE-IND-sID-CPA secure and Delegatee-IBE-IND-sID-CPA secure for the proxy and delegatee's colluding.*

Proof. Suppose A can attack our scheme, we construct an algorithm B solves the DBDH problem in G. On input (g, g^a, g^b, g^c, T), algorithm B's goal is to output 1 if $T = e(g, g)^{abc}$ and 0 otherwise. Let $g_1 = g^a, g_2 = g^b, g_3 = g^c$.Algorithm B works by interacting with A in a selective identity game as follows:

1. **Initialization**. The selective identity game begins with A first outputting an identity ID^* that it intends to attack.
2. **Setup**.To generate the system's parameters, algorithm B picks $\alpha' \in Z_p$ at random and defines $h = g_1^{-ID^*} g^{\alpha\prime} \in G$. It gives A the parameters $params = (g, g_1, g_2, h)$. Note that the corresponding $master - key$, which is unknown to B, is $g_2^a = g^{ab} \in G^*$.
3. **Phase 1**
   - *"A issues up to private key queries on ID_i"*. B selects randomly $r_i \in {Z_p}^*$ and $k' \in Z_p$, sets $sk_{ID_i} = (d_0, d_1) = (g_2^{\frac{-\alpha'}{ID_i - ID^*}} {(g_1^{(ID_i - ID^*)} g^\alpha)}^{r_i}, g_2^{\frac{-1}{ID_i - ID^*}} g^{r_i})$. We claim sk_{ID_i} is a valid random private key for ID_i. To see this, let $\widetilde{r_i} = r_i - b/ID - ID^*$. Then we have that
     $d_0 = g_2^{\frac{-\alpha'}{ID_i - ID^*}} {(g_1^{(ID_i - ID^*)} g^\alpha)}^{r_i} = g_2^\alpha {(g_1^{(ID_i - ID^*)} g^\alpha)}^{r_i - b/ID - ID*} = g_2^a (g_1^{ID_i} h)^{\widetilde{r_i}}$.
     $d_1 = g_2^{\frac{-1}{ID_i - ID^*}} g^{r_i} = g^{\widetilde{r_i}}$.

- *"A issues up to rekey generation queries on* (ID, ID')*"*. The challenge B chooses a randomly $x \in Z_p^*$, sets $rk_{ID,ID'} = x$ and returns it to A. He also searches in the `user-key-list` for ID', if find no item of (ID', u'), then return "Reject", otherwise he computes $w = \frac{g^{ID}h^{x}}{g^{u'}}$ and make it be public. For the delegatee, he can verify $(g^{ID}h^{x})^{x} = g^{u'}w$. We can see our simulation can always satisfies this. Thus the delegator and delegatee cannot get any useful information from x.
- *"A issues up to re-encryption queries on* (C_{ID}, ID, ID')*"*. The challenge B runs $ReEnc(rk_{ID \to ID'}, C, ID, ID')$ and return the results.

4. **Challenge** When A decides that Phase1 is over, it outputs two messages $M_0, M_1 \in G$. Algorithm B picks a random bit b and responds with the ciphertext $C = (g^c, (g^{\alpha'})^c, M_b \cdot T)$. Hence if $T = e(g,g)^{abc} = e(g_1, g_2)^c$, then C is a valid encryption of M_b under ID^*. Otherwise, C is independent of b in the adversary's view.
5. **Phase2** A issues queries as he does in Phase 1 except natural constraints.
6. **Guess** Finally, A outputs a guess $b' \in \{0, 1\}$. Algorithm B concludes its own game by outputting a guess as follows. If $b = b'$, then B outputs 1 meaning $T = e(g,g)^{abc}$. Otherwise it outputs 0 meaning $T \neq e(g,g)^{abc}$.

When $T = e(g,g)^{abc}$ then A's advantage for breaking the scheme is same as B's advantage for solving DBDH problem. ∎

Theorem 2. *Suppose the DBDH assumption holds, then our scheme is KGC-OW secure for the proxy, delegator and delegatee's colluding.*

Proof. The adversary can only get information about $master - key$ from x, and we know that the KGC chooses a different k for every different user pair (ID, ID'). Even if the adversary know $\frac{u'+k}{\alpha ID+t_2}$ for every (ID, ID'), he can not compute α, t_2 or u', thus our scheme is KGC-OW secure. ∎

5 Discussion

The security model in [16] is not sufficient, they only consider the delegatee's security instead of the delegatee and delegator's security. Furthermore, their model is a typical model of three users(the delegator, the proxy, the delegatee) instead of a multi-user model. In proxy re-encryption, universal compensable security is a proper security notion.

Intuitively, in their scheme, the delegator do not contribute any secret value to the re-encryption key, that means, the proxy can take any user as the delegator, which is obviously contradicted with the goal of proxy re-encryption. Furthermore, why the proxy in their scheme is so powerful is that the KGC has contributed to the re-encryption key with his $master - key$—α via the form of $g^{u'\alpha}$.

On the other hand, the feature of [16]'s scheme maybe is not bad. Actually, there scheme is a anonymous group proxy re-encryption from an IBE group to an IBE user, which maybe can find applications in our life.

Our new scheme is also in the standard model, we can transform it to be a scheme in the random oracle with IND-ID-CCA secure. We note that our scheme can also be transformed to be a IBE-KEM based proxy re-encryption with IND-ID-CCA secure [6].

6 Conclusion

In 2007, Matsuo proposed two types of re-encryption scheme which can re-encrypt the ciphertext from CBE to IBE and IBE to IBE [16]. Now these two schemes are being standardized by IEEEP1363.3 working group[15]. In this paper, we show that their proxy re-encryption scheme from IBE to IBE is not secure. Specially, in their scheme the proxy himself can re-encrypt any IBE user's ciphertext into being a delegatee's ciphertext. We propose a new scheme and prove its security . We also discuss some issues about proxy re-encryption in IBE setting. Although some excellent work has been done in this area[7, 12, 11, 16, 8, 17, 13, 14], but there are still many open problems need to be solved.

References

1. G.Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage.In *ACM Trans. Inf. Syst. Secur. 9 (2006), no. 1, pages 1–30.*
2. M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography.In *Advances in Cryptology - Eurocrypt'98,* LNCS 1403, pp. 127–144.Springer–Verlag,1998.
3. D. Boneh and X.Boyen. Efficient Selective-id Secure Identity Based Encryption without Random Oracles. In *Advances in Cryptology - EUROCRYPT 2004,* LNCS 3027, pp. 223–238. Springer–Verlag, 2004.
4. D. Boneh, E. Goh and T. Matsuo. Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC/submissions/NTTDataProposal-for-P1363.3-2006-09-01.pdf.
5. X.Boyen. Efficient Selective-id Secure Identity Based Encryption without Random Oracles. In *Advances in Cryptology - EUROCRYPT 2004,* LNCS 3027, pp. 223–238. Springer–Verlag, 2004.
6. X.Boyen. The BB_1 Identity-Based Cryptosystem A Standard for Encryption and Key Encapsulation. http://grouper.ieee.org/groups/1363/IBC/submissions/Boyen-bb1-ieee.pdf.
7. R. Canetti and S. Hohenberger, Chosen Ciphertext Secure Proxy Re-encryption.In *In Proceedings of the 14th ACM conference on Computer and Communications Security(CCS 2007)*,pp. 185–194.2007. Also available at Cryptology ePrint Archive: http://eprint.iacr.org/2007/171.pdf.
8. C.Chu and W.Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007,*LNCS 4779, pp. 189–202.Springer–Verlag,2007.
9. S. Hohenberger. Advances in Signatures, Encryption, and E-Cash from Bilinear Groups. Ph.D. Thesis, MIT, May 2006.
10. E. Goh and T. Matsuo. Proposal for P1363.3 Proxy Re-encryption. http://grouper.ieee.org/groups/1363/IBC/submissions/NTTDataProposal-for-P1363.3-2006-08-14.pdf.

11. M. Green and G. Ateniese, Identity-Based Proxy Re-encryption. In *Applied Cryptography and Network Security'07,*LNCS 4521, pp. 288–306.Springer–Verlag,2007.
12. S. Hohenberger, G. N. Rothblum, a. shelat, V. Vaikuntanathan. Securely Obfuscating Re-encryption.In *TCC'07,*LNCS 4392, pp. 233–252.Springer–Verlag,2007.
13. B. Libert and D. Vergnaud, Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption.In *11th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008,*LNCS 4939, pp. 360–379.Springer–Verlag,2008.
14. B. Libert and D. Vergnaud, Tracing Malicious Proxies in Proxy Re-Encryption.In *First International Conference on Pairing-Based Cryptography - Pairing 2008*,Springer–Verlag,2008.
15. L.Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.
16. T. Matsuo, Proxy Re-encryption Systems for Identity-Based Encryption.In *First International Conference on Pairing-Based Cryptography - Pairing 2007,*LNCS 4575, pp. 247–267.Springer–Verlag,2007.
17. J.Shao,D.Xing and Z.Cao, Identity-Based Proxy Rencryption Schemes with Multiuse, Unidirection, and CCA Security.Cryptology ePrint Archive: http://eprint.iacr.org/2008/103.pdf,2008.