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[1]. 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 [10]. Now these schemes are being standardized by IEEEP1363.3 working group[6]. 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.

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, 8, 14],re-encryption schemes in identity based setting [9–12]and re-encryption schemes in hybrid setting[10]. Now the IEEE P1363.3 standard working group is setting up a standard with pairing including re-encryption[6].

In 2007, Matsuo proposed two types of re-encryption scheme which can re-encrypt the ciphertext from CBE to IBE and IBE to IBE [10]. Now these two schemes are being standardized by IEEEP1363.3 working group[6]. 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 [10]. 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[6].

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

- The underlying IBE scheme:
  1. $\mathbf{SetUp_{IBE}(k)}$.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. $\mathbf{KeyGen_{IBE}(mk, parms, ID)}$. Given $mk = g_2^{\alpha}$ and ID with $parms$, pick a random $u \in Z_p^*$. Set $sk_{ID} = (d_0, d_1) = (g_2^{\alpha}(g_1^{ID}h)^u, g^u)$. The KGC preserves a `user-key-list` of form (ID, u) and makes it be secret.
  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. $\mathbf{KeyGen_{PRO}(sk_R, parms, ID, ID')}$. 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').
  3. $\mathbf{ReEnc(rk_{ID \to ID'}, parms, C_{ID}, ID')}$. Given the delegator's identity ID, the delegatee's identity ID', $rk_{ID \to ID'} = (ID \to ID', \frac{u'+k}{\alpha ID + t_2})$,$C_{ID} = (C_1, C_2, C_3)$ 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 $C_{ID'} = (C_1', C_2', C_3') = (C_1, C_2, \frac{C_3 e(C_2^{rk_{ID \to ID'}}, g_1^{(ID'-ID)})}{e(w^{(ID'-ID)}, C_1)}) \in G^2 \times G_1$.
  4. $\mathbf{Check(parms, C_{ID}, ID)}$. 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

$$
\begin{aligned}
\frac{C_3' e(d_1, C_2')}{e(d_0, C_1')} &= \frac{M \cdot e(g_1, g_2)^r e(C_2^{rk_{ID \to ID'}}, g_1^{(ID'-ID)})) e(g^{u'}, (g_1^{ID}h)^r)}{e(w^{(ID'-ID)}, C_1) e(g_2^{\alpha}(g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{M \cdot e(g_1, g_2)^r e((g_1^{ID}h)^{r \frac{u'+k}{\alpha ID + t_2}}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e(g_2^{\alpha}(g_1^{ID'}h)^{u'}, g^r)} \\
&= \frac{M e((g_1^{ID}h)^{r \frac{u'+k}{\alpha ID + t_2}}, g_1^{(ID'-ID)}) e(g^{u'}, (g_1^{ID}h)^r)}{e(g_1^{k(ID'-ID)}, g^r) e((g_1^{ID'}h)^{u'}, g^r)}
\end{aligned}
$$

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

Our scheme is a secure proxy re-encryption from IBE to IBE based on BB1, we give the theorem as following

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

We will give the security proof in the near future.

5 Discussion

The security model in [10] 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 $g^{u'\alpha}$.

When considering proxy re-encryption in IBE settings, previous work just think generating re-encryption key by the delegator and the delegatee, but we know that the KGC plays an important role in the IBE(or IBS) setting. So can we design schemes with re-encryption key generated by the delegator, the KGC and the delegatee? That's maybe a good research direction.

On the other hand, the feature of [10]'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.

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 [10]. Now these two schemes are being standardized by IEEEP1363.3 working group[6]. 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 predefined delegatee's ciphertext. We propose a rescue scheme and discuss some issues about proxy re-encryption in IBE setting. Although some excellent work has been done in this area[7–14], but there are still many open problems need to be solved.

References

1. 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.
2. 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.*
3. S. Hohenberger. Advances in Signatures, Encryption, and E-Cash from Bilinear Groups. Ph.D. Thesis, MIT, May 2006.
4. 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.
5. 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.
6. L.Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.
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. S. Hohenberger, G. N. Rothblum, a. shelat, V. Vaikuntanathan. Securely Obfuscating Re-encryption.In *TCC'07,*LNCS 4392, pp. 233–252.Springer–Verlag,2007.
9. 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.
10. 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.

11. C.Chu and W.Tzeng. Identity-based proxy re-encryption without random oracles. In *ISC 2007,*LNCS 4779, pp. 189–202.Springer–Verlag,2007.
12. 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.
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.