Analysis on the Security of an Identity Based Proxy Re-encryption

Xu an Wang and Xiaoyuan Yang
Key Laboratory of Information and Network Security
Engneering College of Chinese Armed Police Force, P. R. China
E-mail:wangxahq@yahoo.com.cn, wangxuaan@gmail.com

Abstract— **In Pairing'07, Matsuo proposed two proxy re-encryption schemes: proxy re-encryption from CBE to IBE and IBE to IBE. Now both of the schemes have been standardized by P1363.3 workgroup. In this paper, we show that the proxy re-encryption scheme from IBE to IBE is not as secure as its author claimed. We give two attacks to this scheme. The first attack shows that the proxy can re-encrypt any IBE user's ciphertext to be the delegatee's ciphertext. The second attack implies that, if the proxy colludes with any delegatee, the proxy and this delegatee can derive any other IBE user's secret key.**

I. Introduction

The concept of proxy re-encryption comes from the work of Blaze et al. in 1998 [2]. The goal of proxy re-encryption 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 proxy re-encryption schemes and discussed its several potential applications [1]. In ACNS'07, Green et al. proposed the first identity based proxy re-encryption schemes [6]. In Pairing'07, Matsuo proposed new proxy re-encryption schemes in identity based setting [8]. Interestingly, they proposed the concept of four types of proxy re-encryption: IBE to IBE, IBE to CBE, CBE to CBE and CBE to IBE, which can help the ciphertext circulate smoothly in the network. They constructed two proxy re-encryption schemes: one is the hybrid proxy re-encryption from CBE to IBE, the other is the proxy re-encryption from IBE to IBE. Now both of the schemes have been standardized by P1363.3 workgroup [7].

In this letter, we show that Matsuo's proxy re-encryption from IBE to IBE [1] is not as secure as its author claimed. We first review the definition and security model for identity based proxy re-encryption proposed by Matsuo in Pairing'07, and then we review their scheme. At last we give two attacks to their scheme in their security model.

II. Review of Identity Based Proxy Re-encryption Proposed in Pairing'07

A. Definition and Security Model

There are five entities involved in an identity based proxy re-encryption system, delegator, proxy, delegatee, PKG and *Re-encryption Key Generator* RKG [2].

[1]Proxy re-encryption scheme from IBE to IBE is actually the identity based proxy re-encryption scheme.

[2]The PKG and the RKG might be operated by one entity.

Definition 1: An identity-based proxy re-encryption system consists of: 1)the four algorithms making up an IBE system $\mathsf{SetUp}_{\mathsf{IBE}}$, $\mathsf{KeyGen}_{\mathsf{IBE}}$, $\mathsf{Enc}_{\mathsf{IBE}}$, and $\mathsf{Dec}_{\mathsf{IBE}}$,2)and five algorithms for re-encryption, which are

1) $\mathsf{EGen}(sk_{\mathsf{ID}}, \mathsf{params})$. Given an IBE secret key sk_{ID} for ID with params, generate e_{ID} for re-encryption key generation.
2) $\mathsf{KeyGen}_{RKG}(\mathsf{mk}, \mathsf{params})$. Given an IBE master-secret key mk with params, generate a secret key sk_R for re-encryption.
3) $\mathsf{KeyGen}_{PRO}(sk_R, e_{\mathsf{ID}'}, \mathsf{params}, \mathsf{ID}, \mathsf{ID}')$. Given sk, $e_{\mathsf{ID}'}$, the delegator's identity ID and the delegatee's identity ID' with params, generate a re-encryption key $rk_{\mathsf{ID}\to\mathsf{ID}'}$.
4) $\mathsf{ReEnc}(rk_{\mathsf{ID}\to\mathsf{ID}'}, \mathsf{params}, C_{\mathsf{ID}}, \mathsf{ID}, \mathsf{ID}')$. Given the delegator's identity ID, the delegatee's identity ID', the re-encryption key $rk_{\mathsf{ID}\to\mathsf{ID}'}$, and an IBE ciphertext C_{ID} with params, re-encrypt C_{ID} into the different IBE ciphertext $C_{\mathsf{ID}'}$.
5) $\mathsf{Check}(\mathsf{params}, C_{\mathsf{ID}}, \mathsf{ID})$. Given the delegator's identity ID and an IBE ciphertext C_{ID} with params, output 0 if C_{ID} is a malformed ciphertext for ID. Otherwise, output 1.

Furthermore, the PKG deploys the digital signature scheme (KeyGen_{Σ}, Sign, Verify) to sign e_{ID} for authenticating e_{ID}.

Definition 2: IND-ID-CPA security for identity based proxy re-encryption is defined as a game between the adversary $\mathcal{A}$ and challenger $\mathcal{C}$ like following:

Setup The challenger $\mathcal{C}$ selects a digital signature scheme (KeyGen_{Σ}, Sign, Verify). $\mathcal{C}$ generates

1) $(sk_{\Sigma}, vk_{\Sigma})$ by running KeyGen_{Σ},
2) (params, mk) by running $\mathsf{SetUp}_{\mathsf{IBE}}$ and
3) sk_R by running $\mathsf{KeyGen}_{\mathsf{RKG}}$. $\mathcal{C}$ gives (params, vk)to $calA$, keeping (mk, sk_{Σ}, sk_R)to itself.

$\mathsf{Phase\ 1}$ Given (params, vk_{Σ}), $\mathcal{A}$ adaptively queries $\mathcal{C}$. When $\mathcal{A}$ queries $\mathcal{C}$, it responds as following:

- $\mathsf{Secret\ key\ queries}$. When $\mathcal{A}$ queries $\mathcal{C}$ at a point ID, $\mathcal{C}$ generates a secret key sk_{ID_i} for ID by running $\mathsf{KeyGen}_{\mathsf{IBE}}$. $\mathcal{C}$ computes e_{ID_i} by running EGen with the input sk_{ID_i}. $\mathcal{C}$ generates a signature σ_{e_i} for $ID_i||e_{\mathsf{ID}_i}$ by running Sign, and $\mathcal{C}$ returns(sk_{ID_i}, $\mathsf{ID}_i||e_{\mathsf{ID}_i}$, σ_{e_i})to $\mathcal{A}$.
- $\mathsf{Type\text{-}1\ re\text{-}encryption\ key\ queries}$. When $\mathcal{A}$ queries $\mathcal{C}$ about $ID_i \to ID_i'$, $\mathcal{C}$ generates an IBE secret key $sk_{\mathsf{ID}'}$

by running $KeyGen_{IBE}$, and computes $e_{ID'_i}$ by running EGen with the input $sk_{\mathsf{ID}'}$. $\mathcal{C}$ generates a signature $\sigma_{e'_i}$ for $ID'_i||e_{ID'_i}$ by running Sign. $\mathcal{C}$ runs KeyGen_{PRO} with the inputs $e_{ID'_i}$,and returns the resulting re-encryption key $rk_{ID_i \to ID'_i}$ with $(ID'_i, e_{ID'_i})$ to $\mathcal{A}$.

- Type-2 re-encryption key queries. Suppose that $\mathcal{A}$ queries $\mathcal{C}$ about $(ID_i \to ID'_i,\ ID'_i||e_{ID'_i},\ \sigma_{e'_i})$. If$(ID'_i||e_{ID'_i}, \sigma_{e'_i})$ has already generated in the answering for secret key query, then $\mathcal{C}$ rejects the query. Otherwise $\mathcal{C}$ verifies$(ID'_i||e_{ID'_i}, \sigma_{e'_i})$ by running Verify with vk_σ and works as following;
    1) If it is valid then $\mathcal{C}$ runs KeyGen_{PRO} with the input $e_{ID'_i}$,and returns the resulting re-encryption key $rk_{\mathsf{ID}_i \to \mathsf{ID}'}$.
    2) Otherwise $\mathcal{C}$ rejects the query.
- Re-encryption queries. Suppose that $\mathcal{A}$ queries $\mathcal{C}$ about $(sk_{\mathsf{ID}'_i}, C_{ID_i}, ID_i \to ID'_i)$. If $sk_{ID'}$ has never issued to $\mathcal{A}$ then $\mathcal{C}$ rejects the query. Otherwise, $\mathcal{C}$ runs Check with the input(params, C_{ID_i}, ID_i).
    1) If Check outputs 0 then $\mathcal{C}$ rejects the query.
    2) Otherwise, $\mathcal{C}$ generates $e_{\mathsf{ID}'_i}$ by running EGen with $sk_{\mathsf{ID}'_i}$ as input. $\mathcal{C}$ generates $rk_{\mathsf{ID}_i \to \mathsf{ID}'}$ by running KeyGen_{PRO} with the input $e_{\mathsf{ID}'_i}$. $\mathcal{C}$ re-encrypts C_{ID_i} into $C_{\mathsf{ID}'_i}$ by running ReEnc with the input $rk_{\mathsf{ID}_i \to \mathsf{ID}'}$. $\mathcal{C}$ returns $C_{\mathsf{ID}'_i}$ to $\mathcal{A}$
- Challenge. After some queries, $\mathcal{A}$ selects two equal length plaintexts $M_0, M_1 \in \mathcal{M}$ and a target identity ID^* which no secret key for ID^* has issued, and sends them to $\mathcal{C}$. Given $(M_0, M_1, \mathsf{ID}^*)$, $\mathcal{C}$ selects $d \leftarrow_R \{0, 1\}$ and computes $C_{\mathsf{ID}^*} = Enc_{IBE}(ID^*, \mathsf{params}, M_d)$. $\mathcal{C}$ returns C_{ID^*} to $\mathcal{A}$.
- Phase 2. $\mathcal{A}$ continues to issue queries as in Phase 1, and $\mathcal{C}$ responds as before except the following case.
    1) If $\mathcal{A}$ makes the secret key query at the point ID^*, then $\mathcal{C}$ rejects.
    2) If $\mathcal{A}$ makes the re-encryption query such that $ID_i = ID^*$, then $\mathcal{C}$ rejects.
- Guess. Finally, $\mathcal{A}$ outputs a guess $d' \in \{0, 1\}$.

The adversary $\mathcal{A}$ wins if $d' = d$. An identity-based proxy re-encryption system is secure in the sense of IND-ID-CPA if $|Pr[d' = d] - 1/2|$ is negligible.

B. Matsuo's Scheme

The underlying IBE scheme (BB_1-IBE scheme): Let $\mathbb{G}$ be a bilinear group of prime order p (the security parameter determines the size of $\mathbb{G}$). Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ be the bilinear map. For now, we assume public keys (ID) is element in Z_p^*. We later extend the construction to public keys over $\{0, 1\}^*$ by first hashing ID using a collision resistant hash $H : \{0, 1\}^* \to Z_p$. We also assume messages to be encrypted are elements in $\mathbb{G}$. The IBE system works as following:

1) SetUp_{IBE}(k). Given a security parameter k, select a random generator $g \in G$ and random elements $g_2, h \in \mathbb{G}$. Pick a random $\alpha \in Z_p^*$. Set $g_1 = g^\alpha$, $\mathsf{mk} = g_2^\alpha$, and params $= (g, g_1, g_2, h)$. Let mk be the master-secret key and let params be the public parameters.
2) $\mathsf{KeyGen}_{IBE}(\mathsf{mk}, \mathsf{params}, ID)$. Given $\mathsf{mk} = g_2^\alpha$ and ID with params, the PKG 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) $\mathsf{Enc}_{IBE}(ID, \mathsf{params}, M)$. 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 $C_{ID} = (g^r, (g_1^{ID}h)^r, Me(g_1, g_2)^r)$.
4) $\mathsf{Dec}_{IBE}(sk_{ID}, \mathsf{params}, C_{ID})$. Given ciphertext $C_{ID} = (C_1, C_2, C_3)$ and the secret key $sk_{ID} = (d_0, d_1)$ with params, compute $M = \frac{C_3 e(d_1, C_2)}{e(d_0, C_1)}$.

The delegation scheme:

1) $\mathsf{EGen}(sk_{ID}, \mathsf{params})$. Given $sk_{ID} = (d_0, d_1) = (g_2^\alpha(g_1^{ID}h)^u, g^u)$ for ID with params, set $e_{ID} = d_1 = g^u$.
2) $\mathsf{KeyGen}_{PKG}(mk, \mathsf{params})$. Given mk $= \alpha$ with params, set $sk_R = \alpha$.
3) $\mathsf{KeyGen}_{PRO}(sk_R, e_{ID'}, \mathsf{params}, ID, ID')$. Given $sk_R = \alpha, e_{ID'} = g^{u'}$ with params, set $rk_{ID \to ID'} = (ID \to ID', g^{u'\alpha})$.
4) $\mathsf{Check}(\mathsf{params}, C_{ID}, ID)$. Given the delegator's identity ID and $C_{ID} = (C_1, C_2, C_3)$ with params, compute $v_0 = e(C_1, g_1^{ID}h)$ and $v_1 = e(C_2, g)$. If $v_0 = v_1$ then output 1. Otherwise output 0.
5) $\mathsf{ReEnc}(rk_{ID \to ID'}, \mathsf{params}, C_{ID}, ID')$. Given identities ID, ID', $rk_{ID \to ID'} = (ID \to ID', g^{u'\alpha})$, $C_{ID} = (C_1, C_2, C_3)$ with params, the proxy re-encrypt the ciphertext C_{ID} into $C_{ID'}$ as following. First it runs "Check", if output 0, then return "Reject". Else it computes $C_{ID'} = (C'_1, C'_2, C'_3) = (C_1, C_2, C_3 e(C_1^{ID'-ID}, g^{u'\alpha}))$.

III. Attacks

In this section, we give two attacks to this scheme in their security model.

A. Attack I

Suppose adversary $\mathcal{A}$'s target identity is $ID^\star$, he attacks as following:

1) First $\mathcal{A}$ makes secret key query on a randomly chosen identity ID. For $ID \neq ID^\star$, Challenger $\mathcal{C}$ returns $sk_{ID} = (d_0, d_1) = (g_2^\alpha(g_1^{ID}h)^u, g^u)$.
2) Next $\mathcal{A}$ makes Type-1 re-encryption key queries on $\widetilde{ID} \to ID$ where $\widetilde{ID}$ is a randomly chosen identity. For $\widetilde{ID} \neq ID^\star$, Challenger $\mathcal{C}$ returns $rk_{\widetilde{ID} \to ID}$=$(rk_1, rk_2)$=$(\widetilde{ID} \to ID,\ g^{u\alpha})$.
3) When $\mathcal{A}$ receives a ciphertext $C^\star = (C_1^\star, C_2^\star, C_3^\star)$ for $ID^\star$ with params, he re-encrypts this ciphertext to the ciphertext for ID as following. $C_{ID} = (C_1, C_2, C_3) = (C_1^\star, C_2^\star, C_3^\star e({C_1^\star}^{ID-ID^\star}, g^{u\alpha}))$ where $g^{u\alpha}$=rk_2. We can verify this ciphertext is a valid ciphertext for ID.
4) $\mathcal{A}$ can decrypt the ciphertext C_{ID} by the secret key sk_{ID}

for the following.

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

And thus he can decrypt every ciphertext for $ID^\star$.

Remark 1: The first attack shows that the proxy can re-encrypt any IBE user's ciphertext to be the delegatee's ciphertext, which beyond the ability supposed to give proxy, that is, just re-encrypting the delegator's ciphertext to be the delegatee's ciphertext.

B. Attack II

Suppose adversary $\mathcal{A}$'s target identity is $ID^\star$, he attacks as following:

1) First $\mathcal{A}$ makes secret key query on a randomly chosen identity ID. For $ID \neq ID^\star$, Challenger $\mathcal{C}$ returns $sk_{ID} = (g_2^\alpha (g_1^{ID} h)^u, g^u)$ where u is randomly chosen from Z_q^*.
2) Next $\mathcal{A}$ makes Type-1 re-encryption key queries on $\widetilde{ID} \rightarrow ID$ where $\widetilde{ID}$ is a randomly chosen identity. For $\widetilde{ID} \neq ID^\star$, Challenger $\mathcal{C}$ returns $rk_{\widetilde{ID} \rightarrow ID}$=$(rk_1, rk_2)$=$(\widetilde{ID} \rightarrow ID,\ g^{u\alpha})$.
3) Now $\mathcal{A}$ can compute valid private keys for $ID^\star$.

$$\frac{g_2^\alpha (g_1^{ID} h)^u}{g^{u\alpha ID}} \cdot g^{u\alpha ID^\star} = g_2^\alpha (g_1^{ID^\star} h)^u$$

and we can see $(g_2^\alpha (g_1^{ID^\star} h)^u, g^u)$ is a valid private key for $ID^\star$.

Remark 2: The second attack implies that, if the proxy colludes with any delegatee, the proxy and this delegatee can derive any other IBE user's secret key.

IV. Conclusion

In this letter, we give two attacks to an identity based proxy re-encryption [8]. The reason why their scheme is not secure is that their re-encryption key is of the form $g^{u'\alpha}$ where α is the master – key. This re-encryption key can give the adversary more power than just doing re-encryption from the delegator to the delegatee.

V. Acknowledgements

The authors would like to express their gratitude thanks to Dr. Whyte Willam and Dr. Luther Martin for providing us the chance to present this work in the workgroup teleconference.

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] 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.

[6] 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.

[7] L.Martin(editor). P1363.3(TM)/D1, Draft Standard for Identity-based Public Cryptography Using Pairings, May 2008.

[8] 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.