On the Security of Group-based Proxy Re-encryption Scheme

Purushothama B R[1], B B Amberker

Department of Computer Science and Engineering
National Institute of Technology Warangal
Warangal, Andhra Pradesh-506004, INDIA
Email: {puru,bba}@nitw.ac.in

Abstract

Proxy re-encryption (PRE) allows a semi-trusted proxy to convert a ciphertext intended for Alice into a ciphertext for Bob without learning anything about the underlying plaintext. Chunbo Ma et al. have proposed a group based proxy re-encryption scheme to convert a ciphertext from one group to another. Any group member can independently decrypt the ciphertexts encrypted to its group. In their paper, the authors gave a security proof to say that the scheme is secure against adaptive chosen ciphertext attack. However, we highlight the flaws in their scheme and show that their scheme is not secure against adaptive chosen ciphertext attack. In this direction, we construct an adversary who issues only one decryption oracle query and break the security of their scheme with non-negligible advantage.

Keywords: Proxy Re-encryption, Adaptive chosen ciphertext attack, Group proxy re-encryption.

1. Introduction

Proxy re-encryption allows a proxy to convert a ciphertext corresponding to Alice's public key to the ciphertext that can be decrypted by Bob's secret key. Proxy is not fully trusted and does not learn anything about the

[1]Currently the author is with Department of Computer Science and Engineering National Institute of Technology Goa, Farmagudi, Ponda, 403401, Goa, INDIA.

plaintext during conversion. Manbo et al. [1] have introduced the method of delegating decryption right. Blaze et al. [2] proposed the notion of atomic proxy cryptography. Since then, several proxy re-encryption protocols have been proposed [3, 4, 5]. Also, several proxy re-encryption schemes with special functionality have been proposed [6, 7, 8]. The detailed chronological survey of the literature in proxy cryptography can be found in [9].

Ma et al.[10] have proposed a scheme to ensure the privacy of the messages among the group members. In their scheme, anyone can encrypt the message to the group and any member of the group can decrypt the ciphertext. Chunbo Ma and Jun Ao [11] have proposed a bidirectional group-based proxy re-encryption scheme. In their scheme, a message encrypted for group A can be re-encrypted such that the ciphertext can be decrypted by any member of the group B. A proxy can convert the ciphertext of the group A such that members of group B can decrypt the converted ciphertext. The scheme is claimed to be secure against adaptive chosen ciphertext attack.

In this paper, we show that the scheme of Chunbo Ma et al. [11] is not secure against adaptive chosen ciphertext attack. Also, we show that the basic encryption scheme used in group based proxy re-encryption scheme is not secure against adaptive chosen ciphertext attack. We construct an adversary who makes only one decryption query to show that the scheme group based proxy re-encryption scheme is not secure.

2. Chunbo Ma et al's Group Based Proxy Re-encryption Scheme

In this section, we briefly explain Chunbo Ma et al's scheme, security model and construction [11]. We call the scheme in [11] as GPRE scheme. GPRE scheme consists of five algorithms, viz., *KeyGen,ReKeyGen, Enc,ReEnc* and *Dec*.

2.1. Security Notion

The security of the scheme is defined using the following game between the the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$.

- **Setup:** The system is initialized by $\mathcal{C}$ and the resulting system parameters and the public key PK are given to $\mathcal{A}$.
- **Query Phase 1:** In this phase, $\mathcal{A}$ can make Decrypt and Re-encrypt queries.

- **Challenge Phase:** $\mathcal{A}$ chooses and sends two equal length messages M_0 and M_1 to $\mathcal{C}$. $\mathcal{C}$ chooses $e \in \{0,1\}$ and encrypts M_e and sends the corresponding ciphertext C^* to $\mathcal{A}$.

- **Query Phase 2:** In this phase, $\mathcal{A}$ adaptively issues Decrypt and Re-encrypt queries with the restriction that challenge ciphertext C^* is not used in any queries.

- **Guess Phase:** After Query Phase 2, $\mathcal{A}$ outputs $\hat{e} \in \{0,1\}$. $\mathcal{A}$ wins the game if $\hat{e} = e$.

The GPRE scheme is said to be secure against adaptive chosen ciphertext attack if the advantage $\epsilon = |Pr[e = \hat{e}] - \frac{1}{2}|$ is negligible.

2.2. Chunbo Ma et al's. GPRE scheme

Let G_1 and G_2 be the cyclic multiplicative groups of order q and g be the generator of G_1. Let $e : G_1 \times G_1 \to G_2$ be the efficiently computable bilinear map. PKG chooses uniformly at random $a, b \in \mathbb{Z}_q^*$ and $h \in G_1$ and computes $g_1 = g^a$ and $g_2 = g^b$. The master private keys are a and b and master public keys are g_1, g_2 and h. The scheme assumes existence of two groups A and B.

- *KeyGen*: PKG chooses $k \in \mathbb{Z}_q^*$ uniformly at random as tag for group A and computes the public keys $PK_{A_1} = g_1^k$, $PK_{A_2} = g_2^k$ for group A. The private key of the member $p_i \in A$ is generated as follows.

  1. PKG chooses $r_i \in \mathbb{Z}_q^*$ uniformly at random.
  2. Computes and outputs the private key $d_i = \{d_{i1}, d_{i2}, d_{i3}\}$ as follows.

  $$d_{i1} = h^{r_i} \cdot g^{k \cdot r_i}, \quad d_{i2} = h^{(r_i - k^{-1})b^{-1}} \cdot g^{a \cdot k \cdot r_i b^{-1}}, \quad d_{i3} = g \cdot h^{r_i}$$

  PKG chooses $l \in \mathbb{Z}_q^*$ uniformly at random as tag for group B and computes the public keys $PK_{B_1} = g_1^l$, $PK_{B_2} = g_2^l$ as public keys for B. The private keys of the members of $p_i \in B$ are similarly computed as explained above.

- *Enc:* To encrypt a message $M \in \{0,1\}^\lambda$ for the group A, the sender chooses $s \in \mathbb{Z}_q^*$ uniformly at random and computes the ciphertext $c = (c_1, c_2, c_3)$ such that,

$$c_1 = M \cdot e(g_1, PK_{A_1})^s, \quad c_2 = (h \cdot PK_{A_1})^s, \quad c_3 = (PK_{A_2})^s$$

- *ReKeyGen:* PKG computes the re-encryption keys as below and gives it to proxy.

$$Key^1_{A\leftrightarrow B} = g^{(\frac{l-k}{k})},^2 \quad Key^2_{A\leftrightarrow B} = ab^{-1}, \quad Key^3_{A\leftrightarrow B} = \frac{l}{k}$$

- *ReEnc:* Proxy re-encrypts the ciphertext $c = (c_1, c_2, c_3)$ of group A to group B using the re-encrypt keys as below.

$$\tilde{c_1} = c_1 \cdot e(c_3, (Key^1_{A\leftrightarrow B})^{Key^2_{A\leftrightarrow B}}), \quad \tilde{c_3} = (c_3)^{Key^3_{A\leftrightarrow B}},$$
$$\tilde{c_2} = \frac{c_2 \cdot c_3^{(Key^2_{A\leftrightarrow B})(Key^3_{A\leftrightarrow B})}}{(c_3)^{Key^3_{A\leftrightarrow B}}}$$

  $\tilde{c} = (\tilde{c_1}, \tilde{c_2}, \tilde{c_3})$ is the re-encrypted ciphertext.

- *Dec:* After receiving the re-encrypted ciphertext $\tilde{c} = (\tilde{c_1}, \tilde{c_2}, \tilde{c_3})$ the member $p_i \in$ B can decrypt the ciphertext as below.

  1. Compute $T = \frac{e(\tilde{c_2}, d_{i3})e(\tilde{c_3}, d_{i2})}{e(\tilde{c_2}, d_{i1})}$
  2. Compute $M = \frac{\tilde{c_1}}{T}$

  The users of group A can obtain the plaintext M from $c = (c_1, c_2, c_3)$ similarly by computing as explained above.

3. Comment on the Security of Chunbo Ma et al.'s scheme

The authors of [11] claim that their group based proxy re-encryption scheme is secure against adaptive chosen ciphertext attack. But, we show that it is indeed not secure. In their security model, the decryption queries are not answered by the challenger $\mathcal{C}$ by following the *Dec* algorithm of the scheme. We construct an adversary $\mathcal{A}$ whose decryption queries are answered by following the decryption procedure of the security model and the *Dec* algorithm of their construction.

[2] In [11], the key is computed as $Key^1_{A\leftrightarrow B} = g^{(\frac{k-l}{k})}$. This key wont decrypt the ciphertext correctly.

3.1. Security Game of Chunbo Ma et al.'s Scheme

Refer Theorem 1 in [11].

- Challenger $\mathcal{C}$ is given $g^a, g^{a \cdot s}, g^{a \cdot k} \in G_1$ and $T \in G_1$. We are interested in the parameters which the $\mathcal{C}$ gives to adversary $\mathcal{A}$.
- $\mathcal{C}$ initializes the system by choosing $w, v \in \mathbb{Z}_q^*$ uniformly at random and publishing the following parameters:

$$g_1 = g^a, \;\; g_2 = g^{a \cdot w}, \;\; PK_{A_1} = g^{a \cdot k}, \;\; PK_{A_2} = g^{a \cdot k \cdot v}, \;\; h = g^{a \cdot k \cdot w}$$

Query Phase 1: We consider only decrypt queries, as our $\mathcal{A}$ uses only decryption queries.

- **Decrypt Queries:** To every new query $c = (c_1, c_2, c_3)$, $\mathcal{C}$ computes and outputs $M = \frac{c_1}{e(g_1, c_3^{\frac{1}{w}})}$.

Challenge Phase: After query phase 1, $\mathcal{A}$ chooses two equal length messages M_0 and M_1 and sends to $\mathcal{C}$. $\mathcal{C}$ chooses a random bit $e \in \{0, 1\}$ and outputs the challenge ciphertext $c^* = (c_1^*, c_2^*, c_3^*)$ such that,
$c_1^* = M_e \cdot e(g_1, T) = M_e \cdot e(g^a, g^{a \cdot k})^{s/a}$

$c_2^* = (T)^{w+1} = (g^{k \cdot s})^{w+1} = (g^{a \cdot k \cdot w} \cdot g^{a \cdot k})^{s/a}$

$c_3^* = (T)^w = (g^{k \cdot s})^w = (g^{a \cdot k \cdot w})^{s/a}$

Query Phase 2: In query phase 2, $\mathcal{A}$ continues to adaptively issue decrypt and re-encrypt queries. $\mathcal{C}$ responds to these queries as in query phase 1. However, query on $c^* = (c_1^*, c_2^*, c_3^*)$ is not permitted.

Guess: $\mathcal{A}$ outputs bit $\hat{e} \in \{0, 1\}$ for e and wins the game if $\hat{e} = e$. The scheme is said to be secure against adaptive chosen ciphertext if $\mathcal{A}$ has negligible advantage $\epsilon = |Pr[e = \hat{e}] - \frac{1}{2}|$.

3.2. Our Adversary Attacking the Chunbo Ma et al.'s Scheme

We construct an adversary who wins the above game with significantly high probability (essentially with probability 1).

Claim 1 (Adversary). *There exists an adversary $\mathcal{A}$ who issues one decryption query in the above game and guesses the bit $\hat{e}$ for e such that $Pr[e = \hat{e}] = 1$ and advantage of the adversary is non-negligible.*

Proof 1. *Challenger $\mathcal{C}$ gives all the public parameters to $\mathcal{A}$. $\mathcal{A}$ does not issue any queries (decrypt or re-encrypt) to $\mathcal{C}$ in query phase 1. $\mathcal{A}$ chooses two equal length messages M_0 and M_1 and sends to $\mathcal{C}$. $\mathcal{C}$ chooses $e \in \{0,1\}$ and encrypts M_e and gives $c^* = (c_1^*, c_2^*, c_3^*)$ to $\mathcal{A}$ such that $c_1^* = M_e \cdot e(g_1, T)$, $c_2^* = (T)^{w+1}$, $c_3^* = (T)^w$. c^* is the challenge ciphertext. After receiving c^*, $\mathcal{A}$ does the following.*

- *$\mathcal{A}$ chooses $t \in \mathbb{Z}_q^*$ uniformly at random.*
- *Chooses a distinct message M_2 such that $M_2 \neq M_0$ and $M_2 \neq M_1$.*
- *Computes $c_1 = (M_2 \cdot c_1^*)^t = M_2^t \cdot M_e^t \cdot e(g_1, T)^t$*
- *Computes $c_2 = (c_2^*)^t = (T)^{(w+1)t}$ and $c_3 = (c_3^*)^t = (T)^{wt}$*

$\mathcal{A}$ sends to $\mathcal{C}$ a decryption query for the ciphertext $c = (c_1, c_2, c_3)$. This is a valid query as $c \neq c^*$. To answer the decrypt query, $\mathcal{C}$ computes the following.

$$\begin{aligned}
\hat{M} &= \frac{c_1}{e(g_1, c_3^{\frac{1}{w}})} \\
&= \frac{M_2^t \cdot M_e^t \cdot e(g_1, T)^t}{e(g_1, ((T)^{wt})^{\frac{1}{w}})} \\
&= \frac{M_2^t \cdot M_e^t \cdot e(g_1, T)^t}{e(g_1, T^t)} \\
&= \frac{M_2^t \cdot M_e^t \cdot e(g_1, T)^t}{e(g_1, T)^t} \\
\hat{M} &= M_2^t \cdot M_e^t
\end{aligned}$$

$\mathcal{C}$ sends $\hat{M}$ to $\mathcal{A}$. $\mathcal{A}$ outputs a bit $\hat{e}$ correctly by computing and checking as below.

- *Adversary outputs 0 if $(\hat{M} \cdot M_2^{-t}) = M_0^t$ else outputs 1.*

Therefore, $Pr[e = \hat{e}] = 1$ and advantage $\epsilon = \frac{1}{2}$. which is non-negligible. So, adversary correctly guesses the bit e with high probability by making only one decryption query to the challenger. Therefore, the scheme is not secure against adaptively chosen ciphertext attack. It should be noted that adversary has not made any re-encrypt queries.

3.3. Remarks

It should be noted that, the basic encryption operation used by the group based proxy re-encryption scheme is not secure against adaptive chosen ciphertext attack and so is the proxy re-encryption. Adversary does not make any re-encryption queries to the challenger. The scheme in [11] still remains insecure against adaptive chosen ciphertext attack even if the decryption query is answered by following the construction of their scheme. To understand this fact, consider the encryption algorithm *Enc*. Suppose adversary has sent two equal length messages M_0 and M_1 to the challenger. Suppose the challenger chooses a bit $e \in \{0, 1\}$ and computes the challenge ciphertext $c^* = (c_1^*, c_2^*, c_3^*)$ such that by construction,

$$c_1^* = M_e \cdot e(g_1, PK_{A_1})^s, \quad c_2^* = (h \cdot PK_{A_1})^s, \quad c_3^* = (PK_{A_2})^s$$

After receiving c^*, adversary chooses $t \in \mathbb{Z}_q^*$ and computes a ciphertext $c = (c_1, c_2, c_3)$ such that,
$c_1 = (c_1^*)^t = M_e^t \cdot e(g_1, PK_{A_1})^{ts}, \quad c_2 = (c_2^*)^t = (h \cdot PK_{A_1})^{st}, \quad c_3 = (c_3^*)^t = (PK_{A_2})^{st}$ and $c \neq c^*$.

When the adversary sends the decryption query with c, challenger returns $\hat{M} = M_e^t$ to adversary. So, adversary can correctly guess the bit e by comparing $\hat{M}$ with M_0^t or with M_1^t.

4. Conclusion

We have proved that the group-based proxy re-encryption scheme of [11] is not secure against adaptive chosen ciphertext attack. We have shown that the basic encryption operation designed is also not secure against adaptive chosen ciphertext attack. We have given an efficient adversary who issues only one decryption query to show that the scheme is indeed not secure.

References

[1] M. Mambo, E. Okamoto, Proxy cryptosystems: Delegation of the power to decrypt ciphertexts, IEICE Trans. Fund. Electronics Communications and Computer Science. E80-A/1:5463 (1997).

[2] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, in: EUROCRYPT, volume 1403 of *Lecture Notes in Computer Science*, Springer, 1998, pp. 127–144.

[3] G. Ateniese, K. Fu, M. Green, S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, ACM Trans. Inf. Syst. Secur. 9 (2006) 1–30.

[4] S. S. M. Chow, J. Weng, Y. Yang, R. H. Deng, Efficient unidirectional proxy re-encryption, in: AFRICACRYPT, volume 6055 of *Lecture Notes in Computer Science*, Springer, 2010, pp. 316–332.

[5] B. Libert, D. Vergnaud, Unidirectional chosen-ciphertext secure proxy re-encryption, IEEE Transactions on Information Theory. 57 (2011) 1786–1802.

[6] L. Fang, W. Susilo, C. Ge, J. Wang, Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search, Theor. Comput. Sci. 462 (2012) 39–58.

[7] J. Shao, Anonymous id-based proxy re-encryption, in: 17th Australasian Conference on Information Security and Privacy (ACISP), volume 7372 of *Lecture Notes in Computer Science*, Springer, 2012, pp. 364–375.

[8] N. Chandran, M. Chase, V. Vaikuntanathan, Functional re-encryption and collusion-resistant obfuscation, in: 9th Theory of Cryptography Conference (TCC), volume 7194 of *Lecture Notes in Computer Science*, Springer, 2012.

[9] J. Shao, Bibliography on proxy re-cryptography, `http://ndc.zjgsu.edu.cn/~jshao/prcbib.htm`, 2013. [Online; accessed 23-July-2013].

[10] C. Ma, Q. Mei, J. Li, Broadcast group-oriented encryption for group communication, Journal of Computational Information Systems. 3 (2007) 63–71.

[11] C. Ma, J. Ao, Group-based proxy re-encryption scheme secure against chosen ciphertext attack, Int. J. Network Security. 8 (2009) 266–270.