International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.355-362
http://dx.doi.org/10.14257/ijsia.2016.10.7.31

Threshold Delegation Scheme Based on Multi-Proxy Re-Encryption

You-Jin Song

Department of Management, Dongguk University
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea
song@dongguk.ac.kr

Abstract

Proxy re-encryption (PRE) is a re-encryption technique to enable decryption of information encrypted with a delegator's public key by using the delegatee's private key. In existing PRE systems, there are restrictions to prevent delegation, delegatee, and proxy collusion. Therefore, a system to adjust the delegated decryption privilege using multi-proxy is required. This study defines a multi-proxy re-encryption technique based on quorum-controlled asymmetric PRE combined with a proxy that exceeds a threshold. Security weakness against collusion between proxy and delegatee can be prvented by applying such a technique, and re-encryption control by multi-proxy becomes possible.

Keywords*: Threshold Delegation, Proxy Re-Encryption, Multi-Proxy, Cloud*

1. Introduction

Sharing and utilizing computing resources as services, rather than physically owning them, is more effective from follow-up management cost aspects, including maintenance and repair. In this regard, such services are offered from various application domains, so for example, doctors and patients can search and read medical information with their own mobile gadgets anywhere, anytime in a medical services environment. Also, an analysis service sensing abnormal symptoms of a specific disease can be received. In addition, communications between doctor and patient, between patients themselves, and between doctors becomes efficient. By combining cloud computing and u-health care, a health cloud service can be offered. Specifically, the health cloud service enables the collection, sharing, and analysis of medical data via links with hospitals from the cloud computing service perspective. For example, a service member can record his/her own health status in real time using a smartphone and the Web. A doctor examines the real-time recorded health information via the health cloud, analyzes the patient's health status thoroughly, and offers an analysis to the patient. Medical data, however, is sensitive information, disclosure of which can be an invasion of privacy. When data are processed in the cloud computing environment, the problem of infringing/invading security/privacy from the exposure of, or threats to, sensitive personal information may occur.

Inside and outside public institutions, the demand for secondary use of personal health information for research and other purposes has recently increased. Secondary use means a patient's personal health data is used for purposes other than treatment. Specifically, it means using personal health information without a direct bearing on treatment.

For instance, let us assume that a researcher from a local non-profit organization wants to look at the records of all patients treated for breast cancer last year. To read/inspect patients' records, the relevant personal information needs to be removed so the researcher cannot identify the patients. To do so, each patient must consent. The researcher needs to receive a waiver from the organizations, allowing the disclosure of records without removing personal information, *e.g.*, for the institutional review board or a privacy commission.

ISSN: 1738-9976 IJSIA

This study proposes a proxy re-encryption system through which medical information can be utilized inside and outside a medical institution from permission of record disclosure, with the institutional review board and/or privacy commission playing a multi-proxy role.

If data are sent to a delegatee through simple re-encryption using the existing proxy re-encryption style, there is a possibility that collusion may occur between the proxy and delegatee, and there can be cases where a judgment cannot be made as to whether delegation to a delegatee is appropriate or not. Actually, collusion between a delegatee and proxy can be prevented by dividing the decryption privilege of a re-encrypted ciphertext using multi-proxy.

2. Related Works

2.1. Bilinear Maps

The bilinear map $e: G_1 \times G_1 \rightarrow G_T$ (G_T is the output space of a bilinear map) has the following properties on two cyclic groups G_1, G_2[1].

· Bilinear: $e(u^a, v^b) \rightarrow e(u, v)^{ab}$ is established on all $u \in G_1$, $v \in G_2$, and all $a \in Z$.

· Nondegenerate: $e(g, g) \neq 1$ on the generator $g \in G_x$ of $G_x(x = 1,2)$.

· Computable: An efficient algorithm computing $e(u, v)$ on all $u \in G_1$ and $v \in G_2$ exists.

2.2. ID-based Cryptography Systems

An ID-based cryptography system is one that uses a receiver's ID upon encryption [1]. It is a system for a cryptogram receiver to decrypt information by drawing a private key from Private Key Generator(PKG). Under the assumption that computation of an assumption problem is difficult, it was proven that it is safe from a chosen plaintext attack in a random Oracle model. The bilinear Diffie-Hellman (BDH) assumption, which becomes the ID-based cryptography system's basis of safety, can be reviewed as follows.

- Decisional BDH Assumption

Set up T∈G $g, g^a, g^b, g^c \in G$ randomly. $\{g, g^a, g^b, g^c, e(g, g)^{abc}\}$ and $\{g, g^a, g^b, g^c, T\}$ cannot be identified with more than 1/2 probability via algorithm within polynomial time.

- Computational BDH Assumption

Set up $g, g^a, g^b, g^c \in G$ randomly. $e(g, g)^{abc}$ cannot be computed via algorithm within polynomial time.

2.3. Proxy Re-encryption Technique

A variety of modes delegating decryption privileges were proposed through proxy re-encryption (PRE) [2][3][4]. PRE is a technique to conduct re-encryption with a re-encryption key so that decryption of information encrypted with the delegator's public key becomes possible using a delegatee's private key. Proxy may prevent the possibility of the delegator's private key being exposed by re-encryption without decryption of the delegator's ciphertext.

2.4. Type- and Identity-based Proxy Re-encryption Techniques [4]

(1) $Setup(k)$: Receive a security parameter k as input, and generate cyclic groups on a bilinear function (G with decile p , $G \times G \rightarrow G_1$). After selecting random generator g on G, select hash function $H_1: \{0,1\}^* \rightarrow G$, $H_2: \{0,1\}^* \rightarrow Z_p^*$. Generate a master key,

$\alpha_i \in Z_e^*$, with random numbers. Then, compute public key $g^{\alpha_i} = pk$, and output public parameter $params$.

- $params = (G, G_1, p, g, H_1, H_2, pk_j)$

(2) $Extract(id)$: After computing public key $pk_{id_i} = H_1(id_i)$ by receiving the input of master key α_1 , public parameter $params$, and $ID \in \{0,1\}^*$, generate private key $sk_{id_i} = pk_{id_i}^{\alpha_1}$.

(3) $Encrypt_1(m, t, id)$: After generating random numbers $r \in_R Z_e^*$, output $c = (c_{i_1}, c_{i_2}, c_{i_3})$.

$$c_1 = g^r, \; c_2 = m \cdot e(pk_{id}, pk)^{r \cdot H_2(sk_{id_i} \| t)}, \; c_3 = t$$

(4) $Pextract(id_i, id_j, t, sk_{id_i})$: This is conducted by a delegator. Output re-encryption key $rk_{id_i \to id_j}$ by inputting id_i , the id of the delegator, id_i , id , and type information t of the delegatee, and the private key sk_{id_i} of the delegator.

$$rk_{id_i \to id_j} = (t, sk_{id_i}^{-H_2(sk_{id_i} \| t)} \cdot H_1(X),$$
$$Encrypt_2(X, id_j))$$

($X \in_R G_1$)

(5) $\mathrm{Preenc}(c_i, rk_{id_i \to id_j})$: This is conducted by proxy. Output re-cryptogram $c = (c_{j_1}, c_{j_2}, c_{j_3})$ by receiving the input of a cryptogram $c = (c_{i_1}, c_{i_2}, c_{i_3})$ and re-encryption key $rk_{id_i \to id_j}$.

$$c_{j_1} = c_{i_1}$$

$$c_{j_2} = c_{i_2} \cdot e(c_{i_1}, sk_{id_i}^{-H_2(sk_{id_i} \| c_{i_4})} \cdot H_1(X)) = m \cdot e(g^{\alpha_1}, pk_{id_i}^{rH_2(sk_{id_i} \| t)}) \cdot e(g^r, sk_{id_i}^{-H_2(sk_{id_i} \| t)} \cdot H_1(X))$$

$$= m \cdot e(g^r, H_1(X))$$

$$c_{j_3} = Encrypt_2(X, id_j)$$

(6) $Decrypt_1(c_{j_2}, sk_{id_j})$: Output m by receiving the input of cryptogram $c = (c_{i_1}, c_{i_2}, c_{i_3})$. Compute m by receiving the input of c_{j_3}.

$$m' = \frac{c_{j_2}}{e(c_{j_1}, H_1(Decrypt_2(c_{j_3}, sk_{id_j})))}$$

$$= \frac{m \cdot e(g^r, H_1(X))}{e(g^r, H_1(X))} = m$$

In the system proposed in this study, the re-encryption key is computed as follows:

$$rk = (pk_1)^{-rH_2(sk_1)} \cdot (pk_2)^r$$

The difference in this system is that re-encryption is conducted using the public keys of a delegator and a delegatee.

2.5. Dynamic Threshold Cryptography[7]

The participants agree to use $GF(p)$ and generator g together.

Compute public key $E = g^d \ (d = \sum_{i=1}^{n} d_i)$ after selecting private key $0 < d \leq p-1$.

Deliver a message $M < p$ to a receiver through encryption, as follows, and compute g^k and $E^k = (g^k)^d$ after selecting random $k \in {}_r Z_c$.

Select a random polynomial expression, where $f(0) = a_0 = k$:

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$

Compute share $c_i = f(x_i) \ i = 1, 2, \ldots, n$ with each participant's eigen value, x_i .

A sender outputs $(g^k, ME^k, t, c_1 e_1^k, c_2 e_2^k, \cdots, c_n e_n^k)$.

Concerning the attribute subset $B(|B| = t)$, granted with the privilege of participants with more than threshold t, each participant computes the value of $k_i = c_i \prod_{\substack{i \neq j \\ i \in B}} \frac{(-x_j)}{(x_i - x_j)} mod \varnothing(p)$ and forwards it to the sender for decryption.

The sender can calculate m , the original message, by calculating the inverse number after computing $\prod_{\substack{i=1 \\ i \in B}} E^{k_i} = E^{\sum_{i \in B} k_i} = E^k \bmod p \prod_{\substack{i=1 \\ i \in B}} E^{k_i} = E^{\sum_{i \in B} k_i} = E^k \bmod p$.

The proposed system is to divide with g^{s_R} , a value computed with a random polynomial expression based on the proxy's ID. After each proxy computes $k_{P_i} = \prod_{\substack{j \neq i \\ P_j \in QS_t}} \frac{-H_2(ID_{P_j})}{H_2(ID_{P_i}) - H_2(ID_{P_j})} \bmod p$, the r_2 ($f(0) = a_0 = r_2$) value is restored through the set of quorum servers with more than threshold k.

3. Proposed System

An ID-based multi-proxy re-encryption technique divides part of the information encrypted with the delegator's ID as a share using multi-proxy's ID.

It generates part of the re-encrypted cryptogram (U´) with a restored value by a certain share, and to re-encrypt it so that the restored part can be decrypted with a delegatee' s private key through a re-encryption key (rk).

3.1. Overview

In Figure 1, a patient (the delegator) computes random to delegate privilege to an institution and an individual (the delegatee), and generates a cryptogram using and . The delegator sends the cryptogram to a policy administrator, and also sends the share value on using the proxies' IDs to the institutional review board and the privacy commission.

When there's agreement on a value exceeding the threshold, the generated value ( ) is sent to the policy administrator, and the re-encrypted cryptogram is generated using , once a final decision is made according to policy. Then, it is sent to the researcher who requested the secondary use. The researcher receiving a re-encrypted cryptogram can decrypt it through his/her own private key.

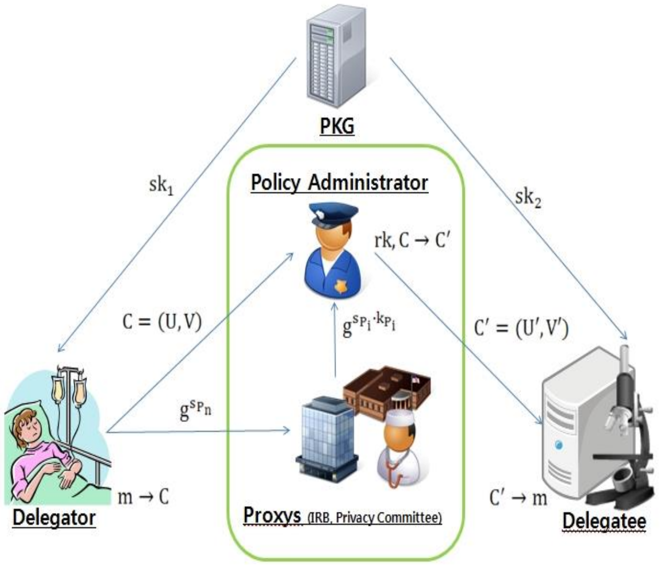

Figure 1. Configuration of the Proposed System

3.2. Details

(1) $Setup(k)$: Input security parameter k , generate cyclic groups on a bilinear function (G , group with decile p and $G \times G \rightarrow G_1$), and select random generator g . Select hash function $H_1 : \{0,1\}^* \rightarrow G$, $H_2 : \{0,1\}^* \rightarrow Z_p^*$.

Generate master key $mk_1 = s \in_R Z_p^*$ with random numbers. Compute public key $g^s = pk$, and reveal public parameter $params$.

- $params = (G, G_1, e, p, g, pk, H_1, H_2)$
- $mk_1 = s$

(2) $Extract(s, params, ID)$: Generate private key $sk_1 = (Q_{ID_1})^s$ after computing public key $pk_1 = Q_{ID_1} = H_1(ID_1)$ by receiving the input of master key s, public parameter $params$, and $ID \in \{0,1\}^*$.

(3) $Split(f(x), r_2, ID_{P_i}, g, H_2)$: This is conducted by a delegator. Generate random $r_1, r_2 \in_R Z_p^*$, and compute r $(r_1 + r_2 = r)$.

Generate a $k-1$ random polynomial expression:

$f(x) = r_2 + f_1 x + f_2 x^2 + \cdots + f_{k-1} x^{k-1}$

where $f(0) = r_2$.

Compute $f(H_2(ID_{P_i})) = s_{P_i}$ (share value of r_2) using $ID_{P_i}(1 \leq i \leq n)$ of the proxies to be shared. After computing $g^{s_{P_i}} = E$, send $g^{s_{P_i}}$ and H_2 to each proxy.

After proxies that exceed threshold k compute k_{P_i} , calculate

$$k_{P_i} = \prod_{\substack{j \neq i \\ P_j \in QS_i}} \frac{-H_2(ID_{P_j})}{H_2(ID_{P_i}) - H_2(ID_{P_j})} \bmod p$$

$E^{k_R} = (g^{s_R})^{k_R}$.

(4) $Encrypt(m, params, pk_1, sk_1, r)$: This is conducted by the delegator. Compute cryptogram C by receiving the input of public parameter $params$, plaintext m , delegator's pubic key $pk_1 = Q_{ID_1}$, private key sk_1 and r :

$$C = (U, V) = (g^{r_1}, m \cdot e(pk_1, pk)^{r \cdot H_2(sk_1)})$$

(5) $RKGen(params, sk_1, pk_1, pk_2)$: This is conducted by the delegator. Compute rk by receiving the input of public key parameter $params$, and sk_1 , pk_1 , and pk_2 :

$$rk = (pk_1)^{-rH_2(sk_1)} \cdot (pk_2)^r$$

(6) $Reconstruct(x_{P_i})$: This is conducted by the quorum sever. Compute the value of E^{k_R} that exceeds the k set of proxies meeting the conditions and that restores g^{r_2} :

$$\prod_{i \in QS_t} E^{k_{P_i}} = g^{\sum_{i \in QS_t}(s_R \cdot k_R)} = g^{\sum_{i \in QS_t} s_i \left(\prod_{i \in QS_t} \frac{-H_2(ID_{P_j})}{H_2(ID_{P_i}) - H_2(ID_{P_j})} \right) \bmod p} = g^{r_2}$$

(7) $Re-encrupt(Params, C, rk, g^{r_2})$: This is conducted by the quorum sever. Compute $C' = (U', V')$ by receiving the input of public parameter $params$, cryptogram C , re-encryption key rk , and restored share value g^{r_2} .

$$U' = U \cdot g^{r_2} = (g^{r_1})(g^{r_2}) = g^{r_1 + r_2} = g^r$$

$$V' = V \cdot e(pk, rk)$$

$$= m \cdot e(pk, pk_1)^{r \cdot H_2(sk_1)} \cdot e(pk, pk_1^{-r \cdot H_2(sk_1)} \cdot (pk_2)^r)$$

$$= m \cdot e(g^s, Q_{ID_1})^{r \cdot H_2(sk_1)} \cdot e(g^s, Q_{ID_1}^{-r \cdot H_2(sk_1)} \cdot (pk_2)^r)$$

$$= m \cdot e(g^s, Q_{ID_1})^{r \cdot H_2(sk_1)} \cdot e(g^s, Q_{ID_1})^{-r \cdot H_2(sk_1)} \cdot e(g^s, (pk_2)^r)$$

$$= m \cdot e(g^s, (pk_2)^r)$$

$$C' = (U', V') = (g^r, m \cdot e(g^s, (pk_2)^r))$$

(8) $Decrypt(params, sk_2, C')$: Decrypt m after computing $e(U', sk_2)$ by receiving the input of public parameter $params$, the cryptogram, and C' and sk_2 :

$$V' / e(U', sk_2)$$

$$= m \cdot e(g^s, (Q_{ID_2})^r) / e(g^r, (Q_{ID_2})^s)$$

$$= m \cdot e(g, (Q_{ID_2}))^{r \cdot s} / e(g, (Q_{ID_2}))^{r \cdot s}$$

$$= m$$

4. Results and Discussion

From the configuration of the ID-based re-encryption technique, when a proxy performs the re-encryption process converting a cryptogram, the proxy must not know the private keys of delegator and proxy. The proxy also should not know the plaintext information of the cryptogram alone. Through collusion between the proxy and delegator, or between the proxy and delegatee, weakness in the system security should not be exposed [5].

The proposed system generates a re-encryption key from randomization of the parameter r combined with Alice's private key and Bob's public key, created by using Alice's ID and Bob's ID, where $r_1 + r_2 = r$. Actually, r_1 is a random value in data encryption, and r_2 is the random value needed for re-encryption, which is sent to the delegatee.

The value restored through the system's secret sharing is simply g^{r_2}. What can be computed from this value is $U = g^{r_1} \cdot g^{r_2}$, part of the re-encrypted cryptogram, and g^{r} is induced. Therefore, V' is needed to compute the complete re-encrypted ciphertext: to calculate V' , rk is necessary. To compute rk , the delegator's private key sk_1 and the r value are required. However, these two values cannot be computed by a proxy group or a third party (hacker). In this regard, there will be no risk to safety upon re-encryption, although the value restored with secret sharing is exposed. The re-encryption key generation by the system excludes weakness to security from a collusion attack between proxy and delegatee through randomization of the public key generated from Bob's ID.

5. Conclusion

This study proposed a system that safely provides the secondary use of medical data by using an ID-based multi-proxy re-encryption technique. As a further task, various sharing schemes, such as an XOR secret-sharing scheme and a secret-sharing system that can be reused, need to be applied for more efficient sharing.

Acknowledgments

This work was supported by the Dongguk University Research Fund of 2016.

References

[1] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing", Proc. of Crypto 2001, LNCS 2139, Springer-Verlag, **(2001)**, pp. 213-229.

[2] M. Green and G. Ateniese, "Identity-based proxy re-encryption", Cryptology ePrint Archive, Report 2006/473, **(2006)**.

[3] Y. Dodis and A. Ivan, "Proxy cryptography revisited", In Network and Distributed System Security Symposium, **(2003)** February.

[4] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "A Type-and-Identity-based Proxy Re-Encryption Scheme and its Application in Healthcare", Lecture Notes in Computer Science, **(2008)**.

[5] DE. Geer and M. Yung, "Split-and-delegate: Threshold cryptography for the masses", Lecture Notes in Computer Science, **(2003)**.

[6] M. Jakobsson, "On quorum controlled asymmetric proxy re-encryption", Lecture notes in computer science, **(1999)**.

[7] H. Ghodosi, J. Pieprzyk and R. Safavi-Naini, "Dynamic Threshold Cryptosystems(A New Scheme in Group Oriented Cryptography)", Proceedings of PRAGOCRYPT, **(2005)**.

[8] Y.-J. Song, "Delegation Scheme based on Proxy Re-encryption in Cloud Environment", Advanced Science and Technology Letters Vol.133 (Information Technology and Computer Science), **(2016)**, pp. 122-126.

Author

YouJin Song, He received a Ph.D. degree in Information Security from Tokyo Institute of Technology, Japan in 1995. He has been a professor at Dongguk Univ. since 1996. His research interests include privacy protection, secret sharing, cloud security and its application, multimedia security.