Delegation Scheme based on Proxy Re-encryption in Cloud Environment

You-Jin Song
Department of Management, Dongguk University, 707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea
{song@dongguk.ac.kr}
Corresponding Author : song@dongguk.ac.kr

Abstract. In existing PRE system, there are restrictions according to disagreement on delegation, delegatee and proxy’s collusion possibility. Therefore a system to adjust decryption privilege delegated to a delegatee using multi-proxy is required. This study defines a multi-proxy re-encryption technique based on quorum controlled asymmetric PRE under the agreement of proxy with more than threshold.

Keywords: Threshold delegation, Proxy re-encryption, Multi proxy, Cloud.

1 Introduction

In and outside of public institutions, the demand for secondary use of personal health information recently increases, due to research purpose and so on. Secondary use means patient’s personal health data is used for the purpose other than treatment. Namely, it means using personal health information without direct bearings with treatment.

For instance, let’s assume that a researcher of a local non-profit organization wants to look at the records of all patients treated for breast cancer last year, since the researcher researches cancer treatment. To read/inspect patients’ records, the relevant personal information needs to be removed so that the researcher cannot identify who the patients are. In doing so, such an act should be consented by each patient. The researcher needs to receive a waiver from the organizations allowing the disclosure of records without removing personal information, such as institutional review board and privacy commission.

This study proposes a proxy re-encryption system through which medical information can be utilized in and outside of a medical institution through the permission of record disclosure by the institutional review board and privacy commission playing a multi-proxy role.
2 Related Research

2.1 Bilinear Maps

The bilinear map $\epsilon : G_1 \times G_1 \rightarrow G_T$ ($G_T$ is output space of bilinear map) has the following properties on two cyclic groups $G_1$, $G_2$.[7]

- **Bilinear:** $\epsilon(u^a, v^b)$ is established on all $u \in G_1$, $v \in G_2$, and all $a, b \in \mathbb{Z}$.
- **Nondegenerate:** $\epsilon(g, g) \neq 1$ on the generator $g \in G_2$ of $G_2\{\alpha = 1, 2\}$.
- **Computable:** An efficient algorithm computing $\epsilon(u, v)$ on all $u \in G_1$ and $v \in G_2$ exists.

2.2 ID-based Cryptography System

ID-based cryptography system[1] is a system using receiver’s ID upon encryption. It is a system for a cryptogram receiver to decrypt by drawing private key from PKG. ID-based cryptography system was proposed by A Shamir in 1984 for the first time. Under the assumption that computation of an assumption problem is difficult, it was proved that it is safe from CAP (chosen plaintext attack) in a random Oracle model. EDH (Bilinear Diffie-Hellman) assumption, which becomes the ID-based cryptography system’s basis of safety, can be reviewed as follows.[7]

- Decisional BDH Assumption
  
  Set $T \in G$ randomly. $\{g, g^2, g^3, \epsilon(g, g)^{2bc}\}$ and $\{g, g^2, g^3, T\}$ cannot be identified with more than $1/2$ probability by algorithm within polynomial time.
- Computational BDH Assumption
  
  Set up $g, g^2, g^3, g^2, g \in G$ randomly. $\epsilon(g, g)^{2bc}$ cannot be computed by algorithm within polynomial time.

2.3 Proxy Re-encryption

A variety of modes delegating decryption privilege are 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 cryptogram encrypted with delegator’s public key becomes possible using delegatee’s private key. Proxy may exclude a possibility of delegator’s private key exposure by re-encryption without decryption of delegator’s ciphertext.
2.4 Dynamic Threshold Cryptography[6]

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

Compute public key $E = a^d (d = \sum_{i=1}^{k} d_i)$ after selecting private key $0 < d \leq p - 1$. Deliver a message $M < p$ to a receiver through encryption as follows, and compute $a^k$ and $E^k = (a^k)^d$ after selecting random $k \in \mathbb{Z}_p$.

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

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

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

A sender outputs $(a^k, ME^k, t, c_1e_1^k, c_2e_2^k, \ldots, c_ne_n^k)$.

Concerning the attributes’ subset $B(\{B\} = t)$ granted with the privilege of participants with more than threshold $t$, each participant computes the value of

$$k_i = c_i \prod_{x \in B \setminus \{x_i\}} \frac{(-x)}{(x - a_i)} \mod p$$

and sends it to the sender for decryption.

The sender can calculate $m$, the original message by calculating the inverse number, after computing

$$\prod_{x \in B} E(x) = E^k \mod p \prod_{x \in B} E(z) = E^k \mod p$$

The proposed system is to divide with $a^k$, value computed with random polynomial expression, based on proxy’s ID. After each proxy computes

$$k_i = \prod_{x \in B \setminus \{x_i\}} \frac{H_2(ID) - H_2(ID)}{H_2(ID) - H_2(ID)} \mod p$$

$r_2(f(0) = a_0 = r_2)$ value is restored through the set of quorum servers with more than threshold $k$.

3 Proposed Scheme

An ID-based multi-proxy re-encryption technique divides part of cryptogram encrypted with delegate’s ID as share using multi proxy’s ID.

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

In Figure 1, a patient (delegator) computes random $r_1 + r_2 = r$ to delegate privilege to an institution and individual (delegate), and generates a cryptogram using $r_1$ and $r$. The delegator sends the cryptogram to a policy administrator, and also sends the share value on $r_2$ using proxies’ IDs to the institutional review board and privacy commission.

When an agreement on the value having more than threshold, send the generated value $(g^{r_2})$ to the policy administrator, generate the re-encrypted cryptogram using $r_k$, once final decision is made according to the policy. And then send it to the researcher who utilizes the secondary use. The researcher receiving the re-encrypted cryptogram can decrypt it through his/her own private key.

4 Conclusions

This study proposed a system utilizing the secondary use of medical data safely 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 re-used, need to be applied for more efficient $r_2$ sharing. A study on differentiation of multi-proxy’s share restoring capacity, namely on proxy stratification by awarding weighted values is planned to be undertaken.
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 Cryp-
2. M. Green and G. Ateniese, Identity-based proxy re-encryption, Cryptology ePrint Archive,
3. Y. Dodis and A. Ivan, Proxy cryptography revisited, In Network and Distributed System
4. L. Ibraimi, Q Tang, P Hartel, W Jonker, A Type-and-Identity-based Proxy Re-Encryption
5. DE: Geer, M Yung, Split-and-delegate: Threshold cryptography for the masses, Lecture
6. M Jakobsson, On quorum controlled asymmetric proxy re-encryption, Lecture notes in
computer science, 1999
7. Hossein Ghodosi, Josef Pieprzyk, Rei Safavi-Naini, Dynamic Threshold Cryptosystems(A
New Scheme in Group Oriented Cryptography), Proceedings of PRAGOCRYPT