Computers and Electrical Engineering 000 (2018) 1–9

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Privacy preserving cloud data sharing system with flexible control☆

Liming Fang[a], Chunpeng Ge[b,*], Zhiqiu Huang[a], Jiandong Wang[a]

[a] *College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[b] *Department of Computer Engineering, Jiangsu University of Technology, Changzhou, China*

ARTICLE INFO

Article history:
Received 28 August 2017
Revised 28 February 2018
Accepted 28 February 2018
Available online xxx

Keywords:
Cloud computing
Privacy preserving
Proxy re-encryption
Broadcast re-encryption
Public key encryption

ABSTRACT

With the development of cloud technology, sharing date between users securely becomes more and more important. Moreover, the cloud server should provide a flexible control on sharing date. This work presents a notion named fuzzy conditional broadcast proxy re-encryption (FC-BPRE), in which a semi-honest proxy can transform a delegator's ciphertext to a new ciphertext for a set of delegatees when the ciphertext satisfies a certain condition set by the delegator. However, the proxy cannot learn any useful information about the underlying plaintext. The proxy can convert a ciphertext, encrypted under a condition set W, to a ciphertext encrypted under a condition set W' using a broadcast re-encryption key, if and only if S and S' are close to each other. We first formalize the notion of FC-PBRE scheme and then proposed a construction.

1. Introduction

Recently, more and more people prefer to remotely store personal date to cloud servers as the cloud servers support storage and computing service as users need. Confidentiality is the basic requirement for data security in the cloud. Encryption is a basic tool for date Confidentiality. In order to ensure the confidentiality of user's data, people may encrypt their data before uploading to the cloud. However, as data is stored in a ciphertext form, the data owner Alice is unable to sharing his data with another user Bob. One may thought that Alice can send her secret key to the cloud server. Using this key, the cloud server can first decrypt Alice's ciphertext to get the plaintext. And then the cloud server can encrypt the plaintext with Bob's public key. On receiving the ciphertext, Bob can decrypt the ciphertext to get the underlying message using his own secret key. Unfortunately, there are two fatal problems with this mechanism. First, if Alice send her private key to the cloud server, then the cloud server can get all of his data. And encryption becomes meaningless. Second, the cloud server needs to first decrypted Alice ciphertext and then encrypted it using Bob's public key.

Proxy re-encryption (PRE), introduced by Blaze et al. [1], is a wonderful solution to this problem. In a PRE scheme, a proxy can directly convert a user's ciphertext to another user's ciphertext without revealing the plaintext. PRE has been used in a lot of situations such as a cloud data sharing system [2], a distributed file system [2], outsourced filtering of encrypted spam [2], email forwarding [1] systems and so on [3–8]. However, in many applications, instead of converting all ciphertext, Alice may only want the proxy to convert ciphertext that satisfies a certain condition. Weng et al. [17] enabled the flexible

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Huimin Lu.
* Corresponding author.
E-mail address: gecp@jsut.edu.cn (C. Ge).

https://doi.org/10.1016/j.compeleceng.2018.02.048
0045-7906/© 2018 Elsevier Ltd. All rights reserved.

control of encrypted ciphertext by introducing the notion of conditional proxy re-encryption (C-PRE). Although, PRE(C-PRE) is useful in many applications, such as corporate email forwarding systems [9], Alice may want to forward Bob'S business emails to more than one colleague other than Bob, maybe the entire company staff. Chu et al. [9] overcame this problem by proposing conditional broadcast proxy re-encryption, where a proxy can transform Alice's ciphertext to a new ciphertext for a set of users; however, as described in [9], the proxy can only convert ciphertexts matching a specific condition. Thus, conditional broadcast proxy re-encryption (C-BPRE) cannot implement a more flexible combination of keywords.

We use the following scenario to illustrator this problem. Considering a Personal Healthy System (PHS), an user Alice's personal healthy data are encrypted with some keywords such as $\mathsf{I}_1 = (\text{“orthopaedics”} \bigwedge \text{“Skindisease”} \bigwedge \text{“Consultant”} \bigwedge \text{“Downtown of Hongkong”})$ before uploading to the cloud. The system then forwards the ciphertext to the doctor by satisfying the requirement I_1. Nevertheless, when the doctor is on vacation, he may want his substitutes to satisfy at least $d(d \le |\ \mathsf{I}_1\ |)$ conditions of I_1. By employing FC-PRE, the doctor can first specify a new access policy I_2, and then generate a re-encryption key rk_{I_1} for his proxy. When the doctor is absent, the proxy can translate the ciphertext to that of one of his substitutes if and only if $|\mathsf{I}_1 \bigcap \mathsf{I}_2| \ge d$. This further demonstrates the need for an FC-BPRE scheme for cloud date sharing with flexible control on ciphertext.

1.1. Related work

The notion of proxy re-encryption was first introduced by Blaze et al.in Eurocrypt98 [1]. They proposed a bidirectional PRE scheme that is chosen-plaintext secure. In a bidirectional PRE scheme, a proxy can transform a ciphertext from Alice to Bob and vice versa. In ACM CCS 2005, Ateniese et al.citeAFGH05 proposed a CPA secure unidirectional PRE scheme using a bilinear map. However, the previous schemes are only chosen-plaintext secure. To overcome this problem, in PKC08, Libert and Vergnaud [12] proposed a replayable CCA secure unidirectional PRE scheme without random oracles and proved its security in the selective model. All previous schemes are only secure in the selective model. To fill this gap, Weng et al. [13] presented the first CCA-secure unidirectional PRE scheme in the adaptive model. In CANS 2008, Deng et al. [14] proposed a bidirectional PRE scheme without pairings. After this work, Shao and Cao [15], as well as Chow et al. [16], proposed unidirectional PRE schemes without pairings.

To achieve flexible control on an encrypted ciphertext, Weng et al. [17] introduced the notion of conditional proxy re-encryption, in which only ciphertexts satisfying specified conditions set by Alice can be re-encrypted. Similarly, Libert and Vergnaud [12] proposed a PRE scheme that supports warrant-based and keyword-based delegation in PKC 2008. In ProvSec 2009, Fang et al. [18] presented an anonymous conditional proxy re-encryption scheme. Later, in 2012, Fang et al. [19] proposed a fuzzy conditional proxy re-encryption scheme that supports an error-tolerance on the conditions. To employ proxy re-encryption in attribute setting, Liang et al. [10] and Ge et al. [11] proposed the notion of ciphertext-policy attribute proxy re-encryption and key-policy attribute-based proxy re-encryption respectively.

However, all previous schemes only allow the proxy to convert Alice's ciphertext for one delegate at a time. The proxy cannot re-encrypt Alice's ciphertext for a set of users at the same time.

This paper is organized as follows. In Section 2, we provide some preliminaries, and in Section 3, we construct our scheme and prove its CCA security. We conclude our paper in Section 4.

2. Preliminaries

2.1. Mapping

Let G and G_T be two multiplicative cyclic groups. A bilinear mapping $e : G \times G \longrightarrow G_T$ satisfying the following conditions [20]:

1. $e(g^u, h^v) = e(g, h)^{uv}$ for all $u, v \xleftarrow{R} Z_p^*$ and $g, h \in G$.
2. $e(g, g) \neq 1$.
3. $e(g, h)$ is computable in polynomial time, $\forall g, h \in G$.

2.2. n-BDHE assumption

Let $e : G \times G \longrightarrow G_T$ be a bilinear map. Given $2n + 2$ elements

$$(h, g, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^n}, g^{\alpha^{n+2}}, \cdots, g^{\alpha^{2n}}, Q) \in G^{2n+1} \times G_T,$$

an adversary has to decide whether $Q \overset{?}{=} e(g, h)^{\alpha^{n+1}}$.

Next we use g_i repents g^{α^i}, an adversary $\mathcal{A}$'s advantage $Adv_{G,\mathcal{A}}^{n-BDHE}$ is defined as

$$\Big|Pr[\mathcal{A}(h, g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, e(g_{n+1}, h)) = 1 \\ -Pr[\mathcal{A}(h, g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, Q) = 1\Big|$$

The n-BDHE assumption holds if $Adv_{G,\mathcal{A}}^{n-BDHE}$ is negligible for all probability polynomial time(PPT) adversary $\mathcal{A}$.

Please cite this article as: L. Fang et al., Privacy preserving cloud data sharing system with flexible control, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.02.048