Pervasive and Mobile Computing 28 (2016) 113–121

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Secure bidirectional proxy re-encryption for cryptographic cloud storage☆

Jun Shao [a,*], Rongxing Lu [b], Xiaodong Lin [c], Kaitai Liang [d]

[a] School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou, Zhejiang, PR China
[b] School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798, Singapore
[c] Faculty of Business and Information Technology, University of Ontario Institute of Technology, Ontario, Canada
[d] Department of Computer Science, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Available online 25 June 2015

Keywords:
Bidirectional proxy re-encryption
Replayable chosen-ciphertext attack
Master secret security
Multi-use
Constant size
Cryptographic cloud storage

ABSTRACT

Bidirectional proxy re-encryption allows ciphertext transformation between Alice and Bob via a semi-trusted proxy, who however cannot obtain the corresponding plaintext. Due to this special property, bidirectional proxy re-encryption has become a flexible tool in many dynamic environments, such as cryptographic cloud storage. Nonetheless, how to design a secure and efficient bidirectional proxy re-encryption is still challenging. In this paper, we propose a new bidirectional proxy re-encryption scheme that holds the following properties: (1) constant ciphertext size no matter how many times the transformation is performed; (2) master secret security in the random oracle model, i.e., Alice (resp. Bob) colluding with the proxy cannot obtain Bob's (resp. Alice's) private key; (3) replayable chosen ciphertext (RCCA) security in the random oracle model. The above three properties are usually required in the cryptographic cloud storage. Furthermore, the proposed new master secret security may be of independent interest, as it is closer to the original desire: delegate the decryption rights while keeping the signing rights.

1. Introduction

Proxy re-encryption (PRE) [1] allows a secure ciphertext transformation in a way that a semi-trusted proxy can use a re-encryption key delegated from Alice (and Bob) to re-encrypt a ciphertext under Alice's public key into a new ciphertext that Bob can decrypt by using his own private key. However, the proxy cannot do any decryption on the ciphertexts of either Alice or Bob. If the re-encryption key can be used to do the re-encryption in both directions, the PRE scheme is called bidirectional; otherwise, it is called unidirectional. Both types of PRE schemes have their own interesting applications. In this work, we shall focus on bidirectional proxy re-encryption (BPRE), as it still encounters many research challenges when applied to practical scenarios.

Among the applications of BPRE [2–10], the cryptographic cloud storage (sharing) [5,10] has become more and more popular. This kind of application usually works in a dynamic environment which requires the PRE scheme to hold multi-usability and constant ciphertext size. In other words, it demands that the transformed ciphertext can be further transformed while the ciphertext size keeps the same.

☆ The extended abstract of this paper appeared at Provsec 2014.

* Corresponding author.
E-mail addresses: chn.junshao@gmail.com (J. Shao), rxlu@ntu.edu.sg (R. Lu), xiaodong.lin@uoit.ca (X. Lin), kliang4-c@my.cityu.edu.hk (K. Liang).

http://dx.doi.org/10.1016/j.pmcj.2015.06.016
1574-1192/

To the best of our knowledge, there are only few BPRE schemes [1,11–13] satisfying the above requirements. However, those previously reported schemes in [1,11,12] suffer from the so-called collusion attack, i.e., Alice (resp. Bob) colluding with the proxy can obtain Bob's (resp. Alice's) private key. In practice, collusion resistance is crucial, especially when Alice (resp. Bob) uses the same private key to perform decrypting and signing, and she (resp. he) wants to delegate the decryption rights while keeping the signing rights. In the applications of cryptographic cloud storage (sharing), the cloud server (acting as the proxy in the BPRE scheme) is assumed to be not colluding with any user in the system. However, as we know, this assumption in the reality is not always true.

In general, the security notion dealing with the collusion attack is called master secret security proposed by Ateniese et al. [14]. Recently, Weng and Zhao [13] proposed two BPRE schemes based on pairings. One is multi-use but with only CPA secure, the other is CCA secure but not multi-use. Meanwhile, it has been showed that replayable chosen ciphertext (RCCA) security is also crucial in the applications of distributed storage [11]. Therefore, in this paper, to address the above challenges, we would like to propose the first scheme with multi-useability, constant ciphertext size, and RCCA security. The proposed BPRE scheme in this paper can (partially) solve the problem in the cryptographic cloud storage (sharing) mentioned above. Furthermore, the proposed BPRE scheme satisfies our new master secret security where Alice (resp. Bob) colluding with the proxy cannot sign messages on behalf of Bob (resp. Alice). This new definition is closer to the original desire for the master secret security, compared to the existing master secret security where Alice (resp. Bob) colluding with the proxy cannot obtain Bob's (resp. Alice's) private key.

1.1. Main differences between the conference version and the current version

The main difference between the conference version [15] and the current version is the security model for the master secret security. In the conference version, the security model only captures the attacks aiming at computing private key, while the security model in the current version captures the attacks aiming at the forgery on signatures. The security obtained in the latter model is stronger than that in the former model, and the latter one is closer to the original desire for the master secret security.

To coordinate the new security model, we made the following changes in this current version.

- We added the definition of Auxiliary Digital Signature to the definition part.
- We added the signing oracle into the security games of the RCCA security and master secret security, and changed the winning requirements in the security game of the master secret security.
- We added a concrete auxiliary digital signature scheme.
- We gave the new security proofs in the new security models.

1.2. Related work

At EUROCRYPT 1998, Blaze, Bleumer and Strauss [1] proposed the first BPRE scheme (named BBS98) base on ElGamal encryption [16]. Later on, Canetti and Hohenberger [11] proposed the first (R)CCA-secure BPRE scheme (named CH07) by using pairings. At PKC 2011, Matsuda, Nishimaki and Tanaka [12] proposed a new pairing-free CPA-secure bidirectional scheme (named MNT10). All of the above schemes hold multi-usability and constant ciphertext size, but they all suffer from the collusion attack. The main reason that the collusion attack works is that the re-encryption key is computed by sk_A/sk_B, where sk_A and sk_B are the private keys of Alice and Bob, respectively. It is easy to see that once sk_A (resp. sk_B) and sk_A/sk_B are put together, sk_B (resp. sk_A) would be revealed.

Recently, Weng and Zhao [13] proposed two new BPRE schemes by using pairings. The first one (named WZ11a) is multi-use, CPA-secure and master secret secure (in the sense of the old definition), and the second one (named WZ11b) is multi-use, CCA-secure, and master secret secure (in the sense of the old definition). To obtain master secret security, the re-encryption key is computed by sk'_A/sk'_B, where sk'_A and sk'_B are not the private keys but the decryption keys of Alice and Bob, respectively. The analogous relations between sk_A and sk'_A can be found in the identity-based encryption [17,18], where the private key generator's master secret key and the user's private key can be considered as the analogies sk_A and sk'_A, respectively. Clearly, knowing sk'_A does not hurt the secrecy of sk_A.

In Table 1, we summarize the existing BPRE schemes in terms of secrecy of message, master secret security, multi useability and their complexity assumptions. From this table, we can see that our proposal would be the only one that can hold the desired properties at the same time.

The rest of this paper is organized as follows. In Section 2, we give the definitions, security models of BPRE. Our new definition of the master secret security is given in this section. Then, we present our proposal in Section 3, including the description, security analysis and computation comparison. Finally, we draw our conclusions in Section 4.

2. Definitions

2.1. Definition of bidirectional proxy re-encryption

Definition 1 (*Bidirectional Proxy Re-Encryption*)**.** A Bidirectional proxy re-encryption scheme is a tuple of probabilistic polynomial time (PPT) algorithms (KeyGen, ReKeyGen, Enc, ReEnc, Dec):