Future Generation Computer Systems 62 (2016) 140–147

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds

Yang Lu *, Jiguo Li

College of Computer and Information, Hohai University, Nanjing, China

HIGHLIGHTS

- This paper proposes a pairing-free certificate-based proxy re-encryption scheme.
- The scheme is proven secure under the classic CDH assumption.
- The scheme is particularly suitable for the computation-limited devices.

ARTICLE INFO

Article history:
Received 29 May 2015
Received in revised form
8 November 2015
Accepted 10 November 2015
Available online 2 December 2015

Keywords:
Public cloud
Data sharing
Certificate-based proxy re-encryption
Bilinear pairing
Chosen-ciphertext security
Random oracle model

ABSTRACT

To assure the confidentiality of the sensitive data stored in public cloud storages, the data owners should encrypt their data before submitting them to the clouds. However, it brings new challenge for us to effectively share the encrypted data in the public clouds. The paradigm of proxy re-encryption provides a promising solution to data sharing as it enables a data owner to delegate the decryption rights of the encrypted data to the authorized recipients without any direct interaction. Certificate-based proxy re-encryption is a new cryptographic primitive to effectively support the data confidentiality in public cloud storages, which enjoys the advantages of certificate-based encryption while providing the functionalities of proxy re-encryption. In this paper, we propose a certificate-based proxy re-encryption scheme without bilinear pairings. The proposed scheme is proven secure under the computational Diffie-Hellman assumption in the random oracle model. Due to avoiding the time-consuming bilinear pairing operations, the proposed scheme significantly reduces the computation cost. Compared to the previous certificate-based proxy re-encryption schemes with bilinear pairings, it enjoys obvious advantage in the computation efficiency, and thus is more suitable for the computation-limited or power-constrained devices.

1. Introduction

Due to the benefits of cloud computing, increasingly more users have been using public cloud storage for data storing and sharing. However, for the widespread adoption of public cloud storage services, public cloud storage should solve the critical issue of data confidentiality. That is, the sensitive data must be secured from the unauthorized accesses. To protect the confidentiality of the sensitive data, a common approach is to encrypt the data before uploading them to the cloud. Since the cloud service provider (CSP) does not know the keys used to decrypt the encrypted data, the confidentiality of the data is assured. However, traditional encryption technique brings many inconveniences for data sharing between different users. To share the encrypted data with a friend, a data owner has to download his data from the storage server, decrypt them, re-encrypt them using his friend's public key and then send the re-encrypted data to his friend or re-upload the re-encrypted data to the cloud. Obviously, this strategy is extremely inefficient due to the heavy overhead at the data owner. In addition, it loses the merit of the public cloud storage. Therefore, how to flexibly share the encrypted data stored in clouds becomes a challenge.

Proxy re-encryption (PRE), introduced by Blaze, Bleumer and Strauss in Eurocrypt'98 [1], offers us an effective solution to encrypted data sharing in clouds. The main goal of PRE is to solve the problem of secure delegation for the decryption right from a delegator to a delegate. In a PRE system, a semi-trusted third party called proxy is employed by the delegator so that it can convert a ciphertext encrypted under the delegator's public key into a new ciphertext of the same message encrypted under the

* Corresponding author.
E-mail addresses: luyangnsd@163.com (Y. Lu), ljg1688@163.com (J. Li).

http://dx.doi.org/10.1016/j.future.2015.11.012
0167-739X/

delegate's public key without learning the underlying message. More specifically, a PRE system works in the following way: the delegator produces a re-encryption key and gives it to the proxy; when receiving a ciphertext intended for the delegator, the proxy uses the re-encryption key to convert it into a ciphertext for the delegate; when receiving the re-encrypted ciphertext, the delegate recovers the underlying message using his own private key. Obviously, PRE can be used as a fundamental building block to implement the secure and effective data sharing applications in clouds. By using a PRE scheme, a data owner can flexibly delegate the decryption rights of his encrypted data to his friends. Moreover, PRE imposes minor overhead on the users as the authorized recipients can obtain the shared data from the cloud directly without direct interaction with the data owners.

From its introduction, PRE has aroused great interest in the academia and numerous PRE schemes have been presented. But, most of them were built over either conventional public-key cryptography (PKC) (*e.g.* [2–7]) or identity-based cryptography (IBC) (*e.g.* [8–12]). It is well known that conventional PKC has the heavy certificate management problem and IBC suffers from the key-escrow problem. By extending PRE into certificateless PKC introduced by Al-Riyami and Paterson [13], Xu et al. [14] put forward the concept of certificateless PRE to overcome the key-escrow problem. In their proposal, each user independently generates a private key by combining a partial private key from a partially trusted authority named key generation center (KGC) with a secret value selected by the user himself. In this way, certificateless PRE solves the key escrow problem. However, as KGC needs to send partial private keys to users over secure channels, the application of certificateless PRE in public clouds may be limited.

To solve the problems in the previous PRE schemes, Sur et al. [15] brought forth the notion of certificate-based PRE (CB-PRE) by extending PRE into certificate-based encryption (CBE) introduced by Gentry [16]. CBE is a new paradigm that has received a growing amount of attention in recent years [17–23]. It has many appealing features as it simultaneously solves the certificate revocation problem in conventional PKC and the key escrow problem in IBC. In CBE, each user generates a public/private key pair and then sends the public key to a trusted certificate authority (CA) to request a certificate. The certificate has all of the functionality of a traditional PKI certificate and is used as a decrypting key. This added functionality supplies an implicit certificate property so that a user needs to use both his certificate and private key to decrypt the received ciphertext, while other users need not be concerned about the status of this user's certificate. Therefore, CBE eliminates the third-party query problem and simplifies the certificate revocation problem in conventional PKC. Furthermore, CBE eliminates both the key escrow problem (as the CA does not know any user's private key) and key distribution problem (as the certificates needn't be kept secret and the CA can send them publicly). As far as we know, three CB-PRE schemes [15,24,25] have been proposed in the literature so far. In [15], Sur et al. formalized the concept and security model of CB-PRE schemes and proposed the first CB-PRE scheme that is proven secure in the random oracle model [26]. Subsequently, another two provably secure CB-PRE schemes were proposed by Li et al. [24] and Lu [25] respectively.

1.1. Our motivation and contribution

The motivation of this paper is to develop a CB-PRE scheme that does not rely on the bilinear pairings. The previous three CB-PRE schemes [15,24,25] are based on the computationally-heavy bilinear pairings. In spite of the advances in the implementation technique [27,28], the bilinear pairing operation is still regarded as the heaviest time-consuming one compared to other cryptographic operations. For example, the computation cost of a bilinear pairing is approximately twenty times higher than that of a scalar multiplication in super-singular elliptic curve group [29,30]. Because the bilinear pairing operations will greatly increase the computation cost of a device, they are immensely disliked by the computation-limited or power-constrained devices, such as smart phone, PDA.

Based on Schnorr's signature scheme [31,32] and Fujisaki and Okamoto's hash-enhanced ElGamal public-key encryption scheme [33], we construct a pairing-free CB-PRE scheme. In the random oracle model, we strictly prove that it achieves chosen-ciphertext security under the hardness assumption of the computational Diffie-Hellman problem. Without bilinear pairing operations, the proposed scheme significantly decreases the computation cost and is more efficient than the previous pairing-based CB-PRE schemes. This good property makes it be particularly suitable to be employed on the computation-limited or power-constrained devices.

1.2. Paper organization

The rest of this paper is organized as follows. In Section 2, we briefly review the definition of elliptic curve group and the related computational assumption. In Section 3, we introduce the definition and security model of CB-PRE. The proposed CB-PRE scheme is described and analyzed in Section 4 and Section 5 respectively. Finally, we conclude our paper in Section 6.

2. Elliptic curve group and computational assumption

In this section, we make a brief review of elliptic curve group and the computational assumption on which the security proof of our CB-PRE scheme is based.

Let p be a prime number. The finite field F_p is comprised of the set of integers $0, 1, 2, \ldots, p-1$ with the following arithmetic operations:

- Addition: If $a, b \in F_p$, then $a + b = r \pmod p$, where $0 \leq r \leq p-1$. This is known as addition modulo p.
- Multiplication: If $a, b \in F_p$, then $a \cdot b = s \pmod p$, where $0 \leq s \leq p-1$. This is known as multiplication modulo p.
- Inversion: If a is a non-zero element in F_p, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in F_p$ for which $a \cdot c = 1 \pmod p$.

Let a, b be two elements such that $\Delta = 4a^3 + 27b^2 \neq 0$ in a prime finite field F_p. An elliptic curve E over F_p (denoted by E/F_p) defined by the parameters a and b is the set of all solutions $(x, y) \in F_p \times F_p$ to the equation $y^2 = x^3 + ax + b$, together with an extra point O at infinity. The set of points on E/F_p forms an abelian group

$$G = \{(x, y) | x,\ y \in F_p \wedge y^2 = x^3 + ax + b\} \cup \{O\}.$$

The point addition "+" in the group G is defined as follows: Let $P, Q \in G$, l_1 be the line connecting P and Q (l_1 be the tangent line to E/F_p if $P = Q$), and R be the third point of intersection of the line l_1 with E/F_p. Let l_2 be the line connecting R and O. Then $P + Q$ is the third point of intersection of the line l_2 with E/F_p, namely $P + Q$ and R are x-axial symmetry points. The scalar multiplication in the group G can be computed as follows:

$$tP = P + P + \cdots + P (t \text{ times}).$$

The security of our scheme is based on the computational Diffie-Hellman (CDH) assumption.

Definition 1. Let G be an elliptic curve group of prime order q. The CDH problem over G is, given a generator P of G and a binary