Information Sciences 462 (2018) 76–92

Contents lists available at ScienceDirect

Information Sciences

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

Certificateless public key encryption with equality test

Haipeng Qu[a], Zhen Yan[a], Xi-Jun Lin[a,*], Qi Zhang[a], Lin Sun[b]

[a] Department of Computer Science and Technology, Ocean University of China, Qingdao, China
[b] College of Liberal Arts, Qingdao University, Qingdao, China

ARTICLE INFO

Article history:
Received 18 April 2017
Revised 17 February 2018
Accepted 8 June 2018

Keywords:
Authorization
Certificateless public key encryption
Key escrow
Equality test

ABSTRACT

In this paper, we present the concept of certificateless public key encryption with equality test (CL-PKEET), which integrates certificateless public key cryptography (CL-PKC) into public key encryption with equality test (PKEET) to solve the key escrow problem of identity-based encryption with equality test (IBEET). In the CL-PKEET scheme, the receiver first computes his private key with the receiver's secret value and the partial private key generated by the key generation center (KGC). The trapdoor is generated with this private key. Then, using the trapdoor, the receiver authorizes the cloud server to test the equivalence between his ciphertexts and others' ciphertexts. We formalize the system model and definition of CL-PKEET, propose the security models by considering four types of adversaries, and then present a concrete CL-PKEET scheme. Our proposal achieves the IND-CCA security against adversaries without trapdoor, and the OW-CCA security against adversaries with trapdoor. Furthermore, compared with IBEET and PKEET, our proposal which has the features of CL-PKC solves certificate management and key escrow problems simultaneously.

1. Introduction

In the cloud era, plenty of cloud services offer a broad set of global computation, analytics, storage, deployment, and application services to help organizations run faster and lower IT costs. Considering the potential risks of privacy disclosure, cryptosystems are introduced to encrypt the private data. In order to preserve users' privacy and meanwhile support searching on the encrypted data, the notion of searchable encryption (SE) was proposed [16]. Based on SE, the well-known public key encryption with keyword search (PEKS) [2,9] was presented as a solution to support keyword searching over ciphertexts without retrieving messages by using the corresponding trapdoors [3]. However, the PEKS is not suitable for the scenarios participated by multiple users in cloud computing since the ciphertexts are encrypted under the identical public key.

A new notion, called public key encryption with equality test (PKEET), was conceived by Yang et al. [24] to support comparing on the encrypted data with respect to different public keys. This primitive can be used to test whether ciphertexts are generated on the same message in outsourced database. Equality test can be defined like that: let C, C' be two ciphertexts encrypted under two different public keys, where $C = Encrypt(M, PK)$ and $C' = Encrypt(M', PK')$, this algorithm can determine if $M = M'$ holds only via comparing C and C'. If it is the case, the algorithm returns 1, or 0 otherwise. Even if the private data are encrypted under different public keys, anyone is able to search data by using the PKEET test function. In some specific scenarios, PKEET, which trivially supports the traditional functionality of PEKS, is an extension of PEKS.

* Corresponding author.
E-mail address: linxj77@163.com (X.-J. Lin).

https://doi.org/10.1016/j.ins.2018.06.025
0020-0255/

PKEET has many interesting applications, for example, partitioning encrypted email [13] and constructing internet-based personal health record (PHR) [18,21]. In an email system, the encrypted emails can be classified into different partitions according to the emails' encrypted keywords. And in a PHR system, the service provider can permit patients to match their encrypted data with those of others. Then the patients with the same illness can get help by exchanging their treatment experiences and mental processes. As all mentioned applications above, the server can check the equality of the provided ciphertexts but learn nothing about the real contents.

However, anyone is able to verify the equality of ciphertexts without any authorization in Yang et al.'s scheme, which violates the data owners' privacy. Hence, several PKEET schemes with authorization mechanism were proposed. Recently, Ma [13] proposed identity-based encryption with equality test (IBEET), which simplifies the certificate management problem of PKEET and supports user-level authorization.

1.1. Related work

IBE/CL-PKC. Deriving the receiver's public key from his identity, formalized by Shamir [17] as identity-based cryptography, is a solution for the certificate management problem of the traditional public key encryption. Based on identity-based cryptography, an important primitive called identity-based encryption (IBE) was presented. Then Boneh and Franklin [4] presented the first practical IBE scheme based on bilinear pairings. Cocks [7] presented a typical IBE scheme based on quadratic residues. IBE is immune to the certificate management problem, such as storage, distribution, verification and revocation. However, it introduces key escrow problem since the receivers' private keys are generated by the key generation center (KGC). Obviously, IBEET exists the key escrow problem as well. To deal with this problem, an important notion, called certificateless public key cryptography (CL-PKC), was presented by Al-Riyami and Paterson [1].

Public key encryption with equality test. Yang et al. [24] first presented the concept of PKEET and their cryptosystem can be used to determine if two messages in outsourced database is equal by checking the corresponding ciphertexts. Then Tang [22] presented a PKEET scheme supporting fine-grained authorization (FG-PKEET), which introduces authorization mechanism for the first time. Tang [21] proposed a notion, called all-or-nothing PKEET (AoN-PKEET), to support user-level authorization by specifying who can independently test the equivalence between two ciphertexts. Tang [23] proposed a two-proxy scheme extended from FG-PKEET to resist the offline message recovery attacks. Later, Ma et al. [15] introduced a significant primitive called public key encryption with delegated equality test (PKE-DET). This primitive allows only the delegated party to verify the equality of ciphertexts in the scenarios participated by multiple users. Huang et al. [10] proposed a public key encryption scheme with authorized equality test (PKE-AET), which strengthens the privacy protection with user-level warrants and cipher-level warrants. Their construction was broken and fixed by Lee et al. [11]. A notion, called public key encryption with equality test supporting flexible authorization (PKEET-FA), was presented by Ma et al. [14] to support four different types of authorization mechanisms. Recently, Ma [13] proposed the concept of IBEET by combining PKEET and IBE [17] to solve the certificate management problem of PKEET. However, the scheme only achieves the OW-ID-CCA security. Lee et al. [12] proposed a semi-generic construction of PKEET, and proposed the first IBEET achieving the IND-ID-CCA security.

1.2. Our contribution

We stress here again that the traditional PKEET exists the certificate management problem and IBEET exists the key escrow problem. We believe that a primitive which has the features of CL-PKC and PKEET could solve both problems simultaneously. Hence, we propose a new primitive, called certificateless public key encryption with equality test (CL-PKEET).

In the CL-PKEET scheme, the receiver first computes his private key with the secret value picked by himself and the partial private key obtained from the KGC. The receiver's trapdoor is generated with his private key. Then, using the trapdoor, the receiver authorizes the cloud server to test his ciphertexts. It is obvious that the key escrow problem of IBEET could be solved in CL-PKEET. The equality testing procedure in CL-PKEET can be briefly described as follows: let C_A and td_A be receiver A's ciphertext and trapdoor, and C_B and td_B receiver B's ciphertext and trapdoor, respectively. Given (C_A, td_A) and (C_B, td_B), the cloud server can check whether or not $M_A = M_B$ holds. Meanwhile, the server learns nothing about the messages M_A and M_B.

The contribution in this paper is listed below:

1. We present the concept of CL-PKEET, which integrates the notion of CL-PKC into PKEET to solve the key escrow problem of IBEET and support user-level authorization.
2. We give the system model and formal definition of CL-PKEET. Moreover, we formalize the security models for CL-PKEET by considering four types of adversaries.
3. We devise a concrete CL-PKEET scheme, which achieves IND-CCA security against adversaries without trapdoor and OW-CCA security against adversaries with trapdoor.

1.3. Organization

In Section 2, we recall the definition of asymmetric bilinear groups and BDH assumption. The system model, the definition and the security models of CL-PKEET are given in Section 3. The proposed scheme is shown in Section 4. And in