Information Sciences 328 (2016) 389–402

Contents lists available at ScienceDirect

Information Sciences

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

Identity-based encryption with outsourced equality test in cloud computing

Sha Ma*

College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong, China

ARTICLE INFO

Article history:
Received 2 November 2014
Revised 10 August 2015
Accepted 31 August 2015
Available online 7 September 2015

Keywords:
Public key encryption
Searchable encryption
Identity-based encryption
Equality test

ABSTRACT

We firstly combine the concepts of public key encryption with equality test (PKEET) and identity-based encryption (IBE) to obtain identity-based encryption with equality test (IBEET). Inheriting the advantage of IBE, IBEET can simplify the certificate management of PKEET with all messages encrypted with the receiver's public identity. In the IBEET scheme, the receiver computes a trapdoor using the secret value for the identity and then sends it to a cloud server for equality test on its ciphertexts with others' ciphertexts. Using this primitive someone with the trapdoor for its identity can delegate out the capability of equality test on its ciphertexts without requiring a central authority to act as a delegator. So it is very suitable for the client with minimal computation resource, e.g, mobile phone. Furthermore, compared with PKEET, it has security improvement since not anyone can perform the test. Therefore, IBEET may have interesting applications in cloud computing, e.g., partition of encrypted emails. We define one-way chosen-ciphertext security against a chosen identity attack (OW-ID-CCA) and propose a construction in bilinear pairing. Finally, extensive security analysis and comparison with related works show that the proposed scheme is proven secure and useful.

1. Introduction

There has recently been interest in "searchable encryption" due to interesting applications in cloud computing era. A searchable encryption scheme allows a third party to search over a client's encrypted data on its behalf without the need of recovering the plaintexts. It enables organizations and individuals to outsource their data in encrypted form and securely delegate search functionalities to the cloud service provider. Mainly, existing works concentrate on keywords search [2,3,7,9–12,15,16,19,23,24,26,29,30,34,35,37,39,40], where a match is determined by whether the keyword encoded in the trapdoor is equal to the plaintext underneath the ciphertext. Additionally, other works study search queries with more complex comparison structures [5,8,14,17], allowing conjunctive, disjunctive, subset and inner product. Recently, as a special type of searchable encryption, public key encryption with equality test (PKEET) [36] has been proposed to check whether two ciphertexts are encryptions of the same message, which can be used to support keywords search on encrypted data trivially. In order to simplify certificate management of PKEET, we firstly combine the concepts of public key encryption with equality test (PKEET) and identity-based encryption (IBE) to obtain identity-based encryption with equality test (IBEET).

IBEET has interesting applications in cloud computing, e.g., partition of encrypted emails. In the following scenario (see Fig. 1), Alice and Bob work in the same company with a cloud email system. For security reasons, all senders produce encrypted emails

* Tel.: +86 13763374669.
E-mail address: martin_deng@163.com, scau.martha@gmail.com

http://dx.doi.org/10.1016/j.ins.2015.08.053
0020-0255/© 2015 Elsevier Inc. All rights reserved.

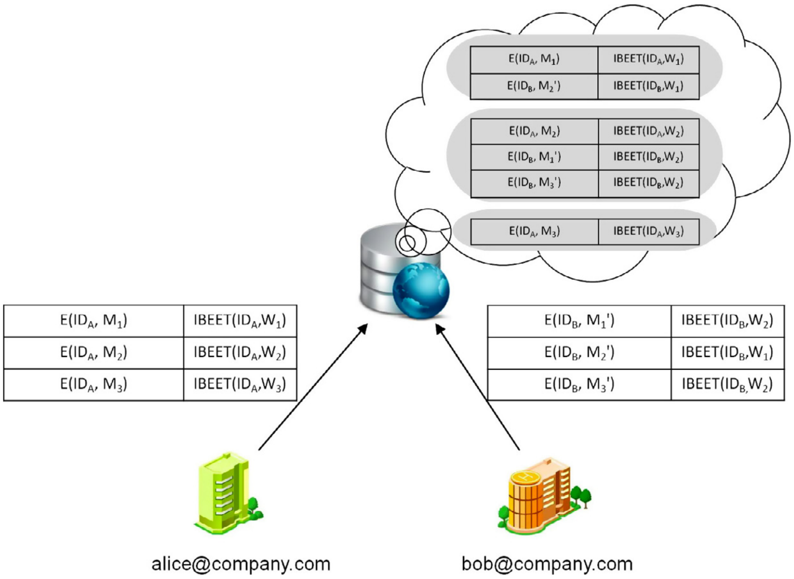
E(ID_A, M_1) | IBEET(ID_A,W_1)
E(ID_B, M_2') | IBEET(ID_B,W_1)
E(ID_A, M_2) | IBEET(ID_A,W_2)
E(ID_B, M_1') | IBEET(ID_B,W_2)
E(ID_B, M_3') | IBEET(ID_B,W_2)
E(ID_A, M_3) | IBEET(ID_A,W_3)
E(ID_A, M_1) | IBEET(ID_A,W_1)
E(ID_A, M_2) | IBEET(ID_A,W_2)
E(ID_A, M_3) | IBEET(ID_A,W_3)
E(ID_B, M_1') | IBEET(ID_B,W_2)
E(ID_B, M_2') | IBEET(ID_B,W_1)
E(ID_B, M_3') | IBEET(ID_B,W_2)
alice@company.com
bob@company.com

Fig. 1. An example of IBEET.

to Alice (Bob) using Alice's (Bob's) public identity: "*alice@company.com*" ("*bob@company.com*") appended with a small number of encrypted keywords, for example, tags about the email's confidentiality including "*Ordinary*", "*Secret*" and "*Top-secret*" could be used as keywords. Suppose that this company expects to utilize the storage partition service of the email system [1] to divide the email storage into different regions according to the customer's requirements depending on whether the emails have the same keywords. In this case, the email server needs to classify all receivers' encrypted emails based on the emails' keywords. Since both the contents of the email and the keywords are encrypted, the email server cannot see the keywords and hence, cannot make the classification of Alice's and Bob's encrypted emails. Thus, our goal is to enable Alice and Bob to authorize the server to perform an equality test on the encrypted keywords in their emails but the server should learn nothing about the emails' contents. Previous works have solved the problem of keywords search on *single* receiver's encrypted emails, but have not studied a general comparison: equality test on *multiple* receivers' keywords in their encrypted emails.

To do so, the sender encrypts his (her) email using a standard public key system with the receiver's identity (ID_A or ID_B), and then appends to the resulting ciphertext an identity-based encryption with outsouced equality test (IBEET) of each keyword. For simplicity, there is only one keyword for each email. To send a message M with keyword W to Alice, the following data are sent to the server:

$$E(\mathsf{ID}_A, M) \,||\, \mathsf{IBEET}(\mathsf{ID}_A, W) \tag{1}$$

The key point of the IBEET scheme is that Alice can give the server a trapdoor td_A to enable it testing whether W is equal to the keyword in others' emails. Given $\mathsf{IBEET}(\mathsf{ID}_A, W)$, td_A, $\mathsf{IBEET}(\mathsf{ID}_B, W')$ and td_B, the server can test whether $W = W'$. If $W \neq W'$, the server learns nothing more about W and W'. Note that although we only refer to two receivers (Alice and Bob) in the example, we hope that the keywords in *multiple* receivers' emails could be compared as long as their trapdoors are given to the server. Besides, we also expect that the IBEET scheme can support keyword search on *single* receiver's encrypted emails trivially, which would help the system upgrade in single user setting.

1.1. Related work

Two related cryptographic primitives have been proposed: public key encryption with equality test [36] and identity-based encryption with keyword search [2].

Public key encryption with equality test. Public key encryption with equality test (PKEET), firstly introduced in [36], is used to check whether two users' ciphertexts contain the same message. To impose authorization on PKEET [36], Tang [31] proposes an enhanced PKEET (FG-PKEET) to realize a fine-grained authorization mechanism, where only the authorized two users can do the test with the help of a trusted party. Also, Tang [33] presents an all-or-nothing PKEET (AoN-PKEET) to achieve a coarse-grained authorization, which specifies who can perform an equality test on ciphertexts. Furthermore, Tang [32] extends FG-PKEET to a two-proxy setting, where two proxies collaborate to execute equality test. Recently, Ma et al. [22] propose a public key encryption with delegated equality test (PKE-DET) to only allow a delegated party to perform the work. Huang et al. [13] present a public key encryption with authorized equality test (PKE-AET), where a receiver authorizes a receiver's warrant on all of its ciphertexts or a receiver authorizes a cipher-warrant on a specific ciphertext. Also, Ma et al. [21] design a flexible PKEET scheme supporting four types of authorization at the same time.