Information Sciences 429 (2018) 349–360

Contents lists available at ScienceDirect

Information Sciences

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

Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes

Willy Susilo[a,*], Guomin Yang[a], Fuchun Guo[a,*], Qiong Huang[b]

[a] School of Computing and Information Technology, University of Wollongong, NSW 2500, Australia
[b] College of Mathematics and Informatics, South China Agricultural University, China

ARTICLE INFO

Article history:
Received 31 December 2015
Revised 14 August 2017
Accepted 17 November 2017
Available online 20 November 2017

Keywords:
Threshold attribute-based encryption
Constant size
Dummy attributes
Provable security

ABSTRACT

Attribute-based encryption (ABE) is an augmentation of public key encryption that allows users to encrypt and decrypt messages based on users' attributes. In a (t, s) threshold ABE, users who can decrypt a ciphertext must hold at least t attributes among the s attributes specified by the encryptor. At PKC 2010, Herranz, Laguillaumie and Ràfols proposed the first threshold ABE with constant-size ciphertexts. In order to ensure the encryptor can flexibly select the attribute set and a threshold value, they use dummy attributes to satisfy the decryption requirement. The advantage of their scheme is that any addition or removal of the attributes will not require any change to users' private keys or public parameters. Unfortunately, the need for dummy attributes makes their scheme inefficient, since the computational cost of encryption is linear to the size of selected attribute set and dummy attribute set. In this work, we improve Herranz et al.'s work, and propose a new threshold ABE scheme which *does not use any dummy attribute*. Our scheme not only retains the nice feature of Herranz et al.'s scheme, but also offers two improvements in comparison to the previous work. Firstly, the computational costs of encryption and decryption are only linear in the size of the selected attribute set. Secondly, without any dummy attribute, most of the computations can be conducted without the knowledge of the threshold t. Hence, threshold change in the encryption phase does not require complete recomputation of the ciphertext.

1. Introduction

As an extension of public key encryption, Attribute-based encryption (ABE) [3,15,24] has been an active area of research recently, since it supports fine-grained access control of the encrypted data. ABE allows users to encrypt and decrypt messages based on user attributes. It is useful in providing anonymous access control, which is a desirable property in many applications, such as encrypted storage in distributed environments. In ciphertext-policy ABE (CP-ABE), a user's private key is generated by the central authority according to his/her attributes. When someone encrypts a message, it selects a policy indicating what attributes the decryptor should hold. Unfortunately, this fascinating functionality comes at a cost. In a typical implementation, the size of a ciphertext is usually proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption.

[*] Corresponding authors.
E-mail addresses: wsusilo@uow.edu.au (W. Susilo), fuchun@uow.edu.au (F. Guo).

https://doi.org/10.1016/j.ins.2017.11.037
0020-0255/© 2017 Elsevier Inc. All rights reserved.

The first CP-ABE scheme with constant-size ciphertexts under AND-gate access structure was proposed in [7]. Subsequently, Herranz, Laguillaumie and Ràfols [16][1] presented the first threshold ABE scheme with constant-size ciphertexts, which supports a more expressive access structure compared to [7]. Their construction works for the (t, s) threshold case, in which a user who is authorized to decrypt should hold at least t attributes among the s attributes selected by the encryptor. Due to the ability of the encryptor to select any threshold value t and attribute set during the encryption phase, their scheme is practical. Their scheme is inspired by the technique introduced by Delerablée and Pointcheval [9] in achieving dynamic threshold identity-based encryption. Herranz et al.'s scheme is proven secure in the standard model based on the hardness of the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) problem [16].

1.1. Motivation

The technique used by Delerablée and Pointcheval [9] is to incorporate some "dummy information" (or, *dummy users* in their identity-based encryption scheme [9]) as part of the computation in order to satisfy the decryption requirement. This technique was then used to construct threshold ABE in [16]. However, the incorporation of dummy attributes in [16] brings efficiency loss in both encryption and decryption, linear in the size of selected attribute set and dummy attribute set. To illustrate the efficiency lost, consider the following parameters used in [16]. Let s be the number of attributes in the chosen attribute set S, t be the threshold and m be the upper bound of the number of attributes in S. The costs for encryption and decryption in [16] are mainly dominated by $m+t+1$ exponentiations and $O(t^2+m)$ exponentiations, respectively. It means, with the choice of small parameters in s and t, we will still require a large computation effort, since m is typically large.

One of the possible application scenarios is the case which usually appears in a Massively Multiplayer Online Game (MMOG). As shown in [25], the recent global epic combat strategy mobile game Clash-of-Clans®[2] is an example of such games which will require an access control mechanism as described in this paper. In this game, each player has multiple attributes which will elevate after gaining more experience in the gameplay. The attributes are the possible *features* in the game, such as {"dragon", "canon", "bomb", $\cdots$}. There is a large set of possible features that a player can acquire during the game, as the set of the possible features is very large. If a player acquires a new feature in the game, it means that this feature has been *authorized* by the central server, otherwise people can just simply cheat by creating the new feature themselves. Occasionally, the central server would like to broadcast a special feature (such as an advanced *weapon* in this game), which will only be available to people who have gained a particular level, which is measured by the number of *features* that this player has acquired. This "offer" will be broadcast to all players, but only players that satisfy the requirement can read this broadcast message. Therefore, this message needs to be sent in an encrypted form. Only players who have satisfied some certain level can decrypt this broadcast message. This certain level is determined by a minimum number of attributes that this player has, and hence, the notion of *threshold* requirement of attributes, t. Referring to the notation that was introduced earlier, the number of possible attributes, S, is typically very large, but a player only has a subset of this set, which is referred to as s. As an example, the set $S=$ {"dragon", "snake", "canon", "bomb", "air trap", $\cdots$}, where typically the total maximum available in S (which is m in the above notation) are around 10,000 features in a single game. A user who has played for a reasonable amount of time will gain approximately 100 features, and hence $s=100$. If the threshold t is set to something like 30, then a user who holds at least 30 out of the possible features will be able to decrypt the broadcast ciphertext. Nevertheless, if the scheme in [16] is used, then each eligible user will still have to conduct a large computation, since m is large. This will make the scheme impractical, especially in the case where the application will be run in a mobile device. We note that in other scenarios, it would be typical to have a large m as well, even the value of s is small.

Although Herranz et al.'s scheme [16] is not very computationally efficient, their construction enjoys a nice feature. Namely, any addition or removal of the attributes will not require any change to users' private keys or public parameters. We note that there are some subsequent works that achieve threshold ABE but do not have this feature. These works will be reviewed in the related work.

1.2. Summary of our contributions

The contributions of this paper are twofold:

- We improve Herranz et al.'s work and propose a threshold ABE scheme which achieves constant-size ciphertexts *without using dummy attributes*. Let s be the number of attributes in the chosen attribute set S, t be the corresponding threshold and m be the upper bound of the number of attributes in S. Compared to our scheme, the major computational cost of encryption of Herranz et al.'s scheme includes $m+t+1$ exponentiations whereas ours requires only $s+3$ exponentiations, and the major computational cost of decryption of Herranz et al.'s scheme includes $O(t^2+m)$ exponentiations, but ours only needs $O(t^s+s)$ exponentiations.
- Another fascinating feature of our scheme is that it supports an efficient threshold change during the encryption process. The impact of using dummy attributes is that the threshold t must be known in the beginning of the encryption process,

[1] The expanded version of this paper appeared in [1].

[2] http://www.supercell.net/games/view/clash-of-clans