Theoretical Computer Science 609 (2016) 49–59

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Efficient dynamic threshold identity-based encryption with constant-size ciphertext

Willy Susilo [*], Fuchun Guo, Yi Mu

Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, NSW 2500, Australia

ARTICLE INFO

Article history:
Received 10 April 2015
Received in revised form 20 June 2015
Accepted 6 September 2015
Available online 10 September 2015
Communicated by G. Persiano

Keywords:
Threshold identity-based encryption
Dynamic
Constant-size

ABSTRACT

This paper revisits the notion of *dynamic threshold identity-based encryption*, due to the recent practical interest. In this notion, an encryptor selects n recipients and a threshold value t for the creation of the ciphertext. The plaintext can only be recovered if at least t receivers cooperate. The key issue in this notion is its *dynamicity*, where after the users enroll to the system, the sender can dynamically select the set of recipients as well as dynamically set the threshold t upon the creation of the ciphertext. Another essential feature of this notion is the need for a constant-size ciphertext. Interestingly, the work by Delerablée and Pointcheval in Crypto 2008 is the only work that achieves this essential feature. In this work, we propose a new scheme achieving all of these nice properties with significant improvements in terms of the computational efficiency (both the encryption and decryption). In our scheme, there is no need to conduct any encryption and decryption using additional dummy users, which are not part of the recipient group, which is in contrast to Delerablée and Pointcheval's work. This improvement has significantly reduced the amount of computations required in both encryption and decryption algorithms.

1. Introduction

The notion of dynamic threshold identity-based encryption (and dynamic threshold public-key encryption) was put forth by Delerablée and Pointcheval [6] in Crypto 2008. The essential feature of this notion is its *dynamicity*, where after the users enroll to the system as possible recipients, the sender can dynamically select the set of recipients as well as dynamically set the threshold t upon the creation of the ciphertext. The case when the dynamicity feature is removed, and hence merely the notion of threshold identity-based encryption (and threshold public-key encryption), has been well studied in the literature (such as [3,4,12,7]). We note that in this notion, the sender cannot determine the set of recipients on the fly as well as dynamically set the threshold t during the creation of the ciphertext.

To be more precise, this notion is described as follows. A message is sent to a dynamic group of users $\{ID_1, ID_2, \cdots, ID_n\}$. It requires at least t users to decrypt the ciphertext. Mostly important, there is *no prekey generation* for this group of users. It means, no new and fresh group key should be generated by the encryptor whenever he/she would like to generate a new ciphertext intended for the group of recipients. We note the threshold value t can be changed every time a new ciphertext is generated, but this does not mean that the encryptor will need to generate a new key as well. Each user

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

http://dx.doi.org/10.1016/j.tcs.2015.09.006
0304-3975/© 2015 Elsevier B.V. All rights reserved.

in this group will merely use their private keys upon the decryption process. An essential requirement of this scheme for practicality reason is due to the constant-size ciphertexts. This will enable the scheme to be used in many applications, such as the classical examples like electronic voting and key-escrow [3], as well as new applications that involve mobile ad-hoc networks and mobile computing [13]. Interestingly, the first and only scheme that achieves constant-size ciphertext in the literature is due to Delerablée and Pointcheval [6] in Crypto 2008. Henceforth, it is an interesting idea on how to improve this scheme.

New application and motivation.
Our work is inspired by the recent globally played mobile game Clash-of-Clans®,[1] which is an epic combat strategy game. Each player can join the game dynamically, and each player is known to the world by his/her identity. Upon joining the system, the player is allocated a password (and hence, this is part of the *KeyGen* algorithm). Each player can join a "clan", either voluntarily or by invitation. In each clan, there is a clan leader, who can declare a war against other clans. This "war declaration" will be created by the clan leader to its clan members, and only if at least t clan members agree to start the war, then they should collaboratively obtain the "war token" issued by the clan leader to declare the war. We note that one may think that this problem can be solved simply using a traditional threshold signature scheme. When the clan member agrees, then he/she will sign on the message and then sends it back to the clan leader. Once a threshold of players is achieved, then the war can be started by the leader. Nevertheless, this will place the bottleneck in the clan leader, and therefore Clash-of-Clan® does not adopt this approach. In this situation, the task of the clan leader is just merely to find a suitable enemy, which has a similar strength. Then, the decision should be directly made by the clan members without going through the clan leader anymore. Therefore, once a threshold of clan members has successfully decrypted the war token, then they can directly start the war without the need to inform the clan leader, who may be busy to find the next target.

We also note that the value of t can vary for each war declaration, as the clan leader will determine the strength of the enemy and based on this information, the value of t is being set. Hence, this leads to the notion of dynamicity. Therefore, the complexity in achieving such a secure mechanism to allow this is due to the dynamicity of the group (and hence, the so-called "clan"). Furthermore, the constant-size ciphertext is part of the requirements as the game should be playable in any mobile device. By having a large size ciphertext, which may be proportional to the number of users, will make the game impractical.

We note that a threshold encryption scheme is *insufficient* to solve the above problem since the value of the threshold has to be able to be determined *on the fly* by the clan leader upon stating the war. Additionally, a new and fresh group key should not be generated for any new group that is selected by the clan leader, even with different values of threshold t. Furthermore, the scheme must be *identity-based* as all the players are only known by their identity in the system. Therefore, the perfect solution for the above application is the notion of dynamic threshold identity-based encryption (DT-IBE).

As mentioned earlier, it is unfortunate that the only candidate that achieves constant-size ciphertext is due to Delerablée and Pointcheval [6] in Crypto 2008. In their scheme, there is a parameter N that denotes the maximum number of group users in the encryption system setting, while n denotes the number of group user. We note that the value N determines the maximum number of users who will play role in the decryption process, and it does not represent the whole users in the system (or it is often referred to as the universe). The computational complexity of their solution (i.e., for encryption and decryption) is $O(N+t)$, where t is the threshold value. This is because in their scheme, the encryptor will be required to "extend" the number of users to reach the upperbound by introducing dummy users. Unfortunately, their solution cannot be employed to solve the above problem, as the additional computation for the dummy users will be quite large if the members of the clan is large.[2] These additional unnecessary computations will be performed by the mobile device that hosts the game, and this will make the battery depletes quickly. Hence, this solution is unacceptable. Therefore, it is clear that a scheme that can perform better than [6], while still maintain all the required features, is highly desirable.

Essential requirements of an ideal dynamic threshold identity-based encryption (DT-IBE) scheme.
Here, we summarize the requirements for an ideal dynamic threshold identity-based encryption (DT-IBE) scheme:

- A DT-IBE scheme is identity-based.
- The value of the threshold in a DT-IBE scheme must be determined on the fly, i.e. during the creation of the ciphertext. Therefore, this value needs to be set by the encryptor.
- A new and fresh group key should not be generated for any new group that is selected by the encryptor, even with different values t.
- A DT-IBE scheme is equipped with a constant-size ciphertext.

To date, only Delerablée and Pointcheval's scheme [6] that achieves all of these requirements. It is unfortunate that the computational complexity of their scheme is $O(N+t)$ as discussed earlier, where it will hinder its adoption in some applications. Therefore, it is desirable to construct a DT-IBE scheme that is equipped with a better computational complexity.

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

[2] We should note that the Clash-of-Clans® game has more than 5 millions daily active users and around 80,000 new installation everyday. The typical size of a clan is around 100 users (and hence, $N = 100$ when we adopt the scheme in [6]).