Theoretical Computer Science 542 (2014) 44–62

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Revocable hierarchical identity-based encryption ☆

Jae Hong Seo [a,*], Keita Emura [b]

[a] Department of Mathematics, Myongji University, Yongin, 449-728, Republic of Korea
[b] National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-kitamachi, Koganei, Tokyo, 184-8795, Japan

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form 21 March 2014
Accepted 27 April 2014
Communicated by G. Persiano

Keywords:
(Hierarchical) identity-based encryption
Revocation
Delegation

ABSTRACT

In practice, revocation functionality is indispensable to the public key cryptosystems since there are threats of leaking a secret key by hacking or legal situation of expiration of contract for using system. In the public key infrastructure setting, numerous solutions have been proposed, and in the Identity Based Encryption (IBE) setting, a recent series of papers proposed revocable IBE schemes. Delegation of key generation is also an important functionality in cryptography from a practical standpoint since it allows reduction of excessive workload for a single key generation authority. Although efficient solutions for either revocation or delegation of key generation in IBE systems have been proposed, an important open problem is efficiently delegating both the key generation and revocation functionalities in IBE systems. Even if the goal is very natural, there are some obstacles to achieve both functionalities at the same time. Libert and Vergnaud, for instance, left this as an open problem in their CT-RSA 2009 paper. In this paper, we propose the first efficient solution for this problem. We prove the selective-ID security of our proposal under the Decisional Bilinear Diffie–Hellman assumption in the standard model.

1. Introduction

The concept of identity-based encryption (IBE) scheme, which is a public key encryption scheme allowing any bit-string (e.g., e-mail address) to be a public key of a user that chooses such a bit-string [26], is introduced by Shamir. Since Boneh and Franklin's first realization of IBE using bilinear pairings over elliptic curves, IBE systems have been applied in numerous applications. Several variations of IBE systems have also been proposed for adding other functionalities. In particular, the hierarchical identity-based encryption (HIBE) scheme allows the key generation center (KGC) to delegate the key generation functionality to users [11] and the revocable IBE (RIBE) scheme allows the KGC to efficiently revoke users for each time period [2].

Revocation functionality in IBE. In public key cryptosystems, we need revocation functionality when a secret key is corrupted by hacking or the period of a contract expires. In the public key infrastructure setting, numerous solutions have been proposed, and in the IBE setting, a series of recent papers has proposed *scalable* RIBE schemes since Boldyreva et al. [2]. In fact, Boneh and Franklin [5] already proposed a trivial solution for revocation functionality, wherein new decryption keys are issued for each time period. However, their solution introduces huge overheads for the KGC that are linearly increased in the number of users. Boldyreva et al. and all subsequent works were aimed at constructing a scalable RIBE scheme, that is, the KGC's overhead increases logarithmically in the number of users. All proposed scalable RIBE schemes used the same methodology for revocation by using a binary tree structure. Each user ID is assigned to a leaf node ζ_{ID} of the binary tree

☆ An extended abstract is presented at the RSA Conference — Cryptographers' Track 2013 [22].
* Corresponding author.

http://dx.doi.org/10.1016/j.tcs.2014.04.031
0304-3975/

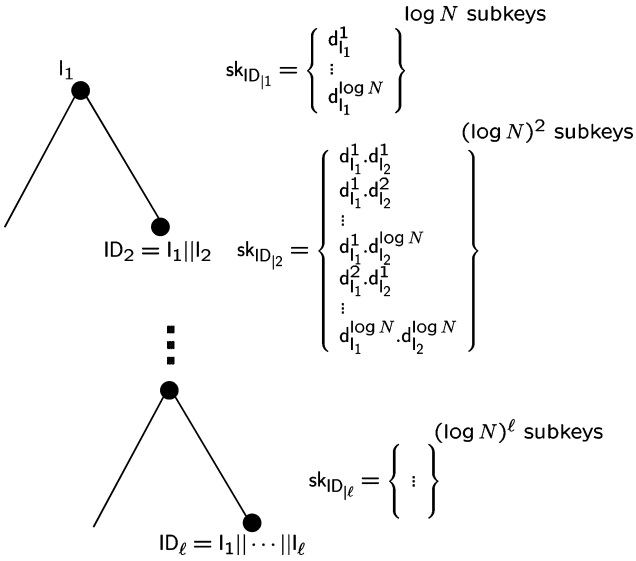

Fig. 1. A trivial construction: Exponentially large secret keys in the corresponding hierarchical level.

structure and has keys corresponding to the nodes on the path between the assigned leaf node and the root node. By using the technique called the Complete Subtree (CS) method [20], which is widely accepted for broadcast encryption, the KGC broadcasts the key update for each time period (i.e., no secure channel is required in this phase) such that only non-revoked users can generate the decryption key for that time period from their secret key and the key update. For a non-revoked user, there is at least one subkey among the $\log N$ size key, where N is the maximum number of users. Since the CS method is secure against colluding and allows short key updates, the resulting RIBE scheme is well scalable and secure.[1]

Delegation functionality in IBE. For a large network, a single KGC has an excessive workload for performing computationally expensive key generation and establishing secure channels to transmit each user's secret key. To mitigate this problem, Horwitz and Lynn [14] introduced the concept of HIBE such that the responsibility for key generation is distributed to the lower-level KGC by delegating key generation functionality. Numerous constructions for HIBE schemes and variants with additional properties have subsequently been proposed [11,3,4,6,10,24,27,16].

Delegation of both key generation and revocation functionalities in IBE – *difficulty*. Although IBE schemes with either efficient revocation or efficient delegation for key generation functionality have been proposed, it is non-trivial to achieve both functionalities at the same time, and in fact Libert and Vergnaud left this as an open problem at CT-RSA 2009 [18]. We simply call such a scheme having both functionalities a Revocable HIBE (RHIBE) scheme. There are some difficulties in achieving RHIBE.

1. Trivial approaches will lead to exponentially large secret keys in the corresponding hierarchical level.
2. Key generations and key updates are recursively defined: this leads some difficulty in the security proof.

All existing scalable RIBE schemes utilize binary tree structures, that is the CS method, for revocation. In the scalable RIBE scheme using the CS method, a secret key of each user consists of $\log N$ subkeys, where N is the number of all users and at least one subkey of a non-revoked user ID can be used to generate a decryption key $\mathsf{dk}_{\mathsf{ID},\mathsf{T}}$ from the key update ku_T on a time period T. If we extend the RIBE scheme for the RHIBE scheme in a natural way, the second-level user has to have $(\log N)^2$ subkeys since one of the subkeys of the parent's key can be used in each time period so that a child should have $\log N$ subkeys for each parent's subkey. In general, ℓ-level users have $(\log N)^\ell$ subkeys, so the size of the secret key exponentially grows in the corresponding hierarchical depth. We illustrate this situation in Fig. 1.

There is another difficulty. For constructing RHIBE, if we follow the same strategy used by all scalable RIBE schemes, KGC may not be able to directly generate secret keys of descendants (except for the first-level user). Each intermediate-level user's secret key is generated according to the shape of the binary tree structure, which is managed by its parent. However, the KGC does not know such a binary tree, so the KGC cannot create secret keys of intermediate-level users. (Note that the KGC can generate decryption keys for all descendants.) Therefore, the secret key and key updates have to be *recursively* defined. This makes the situation more complicated. In particular, in the security model the adversary can query secret keys

[1] The security model for the RIBE scheme is almost equal to that of the conventional IBE scheme. The only difference is that the adversary of the RIBE scheme is allowed to query for the challenge identity ID^*, but in this case the challenge identity should be revoked on the challenge time T^*.