Identity-Based Parallel Key-Insulated Encryption Without Random Oracles: Security Notions and Construction*

Jian Weng[1], Shengli Liu[1,2], Kefei Chen[1], and Changshe Ma[3]

[1] Dept. of Computer Science and Engineering
Shanghai Jiao Tong University, Shanghai 200240, P.R. China
[2] Key Laboratory of CNIS
Xidian University, Xian 710071, P.R. China
[3] School of Computer
South China Normal University Shipai, Guangzhou, 510631, P.R. China
{jianweng, slliu, kfchen}@sjtu.edu.cn, JuanJuansmcs@gmail.com

Abstract. In this paper, we apply the parallel key-insulation mechanism to identity-based encryption (IBE) scenarios, and minimize the damage caused by key-exposure in IBE systems. We first formalize the definition and security notions for ID-based parallel key-insulated encryption (IBPKIE) systems, and then propose an IBPKIE scheme based on Water's IBE scheme. To the best of our knowledge, this is the first IBPKIE scheme up to now. Our scheme enjoys two attractive features: (i) it is provably secure without random oracles; (ii) it not only allows frequent key updating, but also does not increase the risk of helper key-exposure.

Keywords: Parallel Key-Insulation, Identity-Based Encryption, Key-Exposure, Bilinear Pairings.

1 Introduction

1.1 Background and Previous Work

The traditional public key infrastructure involves complex construction of certification authority(CA), and requires expensive communication and computation cost for certification verification. To relieve this burden, Shamir [27] introduced an innovative concept called identity-based cryptography, where user's public-key is determined as his identity such as e-mail address and telephone number. The identity is a natural link to a user, hence it simplifies the certification management in public key infrastructures. The first usable IBE schemes are independently proposed by Boneh and Franklin [3] and Cocks [12], followed by many other elegant IBE schemes (see [2] for some of these). These classical IBE schemes rely on the assumption that secret keys are kept perfectly secure. In

* Supported by the National Science Foundation of China under Grant Nos.60303026, 60403007, 60573030 and 60673077.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 409–423, 2006.

practice, however, it is easier for an adversary to obtain the secret key from a naive user than to break the computational assumption on which the system is based. With more and more cryptographic primitives are deployed on insecure environments (e.g. mobile devices), the key-exposure problem becomes an ever-greater threat. No matter how strong these IBE systems are, once the secret keys are exposed, their security is entirely lost.

In conventional public key encryption scenarios, certificate revocation list (CRL) can be utilized to revoke the public key in case of key-exposure. Users can become aware of other users' revoked keys by referring to the CRL. However, straightforward implementation of CRL will not be the best solution to IBE schemes. Remember that utilizing the CRL, the public key will also be renewed. However, the public key in IBE system represents a user's identity and is not desired to be changed. One exemplification as shown in [22] is the application of IBE systems in a mobile phone scenario, where the phone number represents a user's identity, and it will be simple and convenient for the mobile phone users to identify and communicate with each other only by their phone numbers. Hence renewing the phone number is not a practical solution.

To mitigate the damage caused by key-exposure, several key-evolving protocols have been studied. This mechanism includes forward security [1,5,8], intrusion-resilience [24,13] and key-insulation [15,14]. The latter was introduced by Dodis, Katz, Xu and Yung [15], followed by several elegant key-insulated systems [7,14,11,26,19,22,25,20,29,21,16]. In this model, a physically-secure but computationally-limited device, named base or helper, is involved. The full-fledged secret key is divide into two parts: a helper key and an initial temporary secret key. The former is stored in the helper while the latter is kept by the user. The lifetime of the system is divided into discrete periods. The public key is fixed for all the lifetime, while temporary secret key is updated periodically: at the beginning of each period, the user obtains from the helper an update key for the current period. By combining this update key with the temporary secret key for the previous period, the user can derive the temporary secret key for the current period. Cryptographic operations (such as signing and decryption) in a given period only involve the corresponding temporary secret key in this period. Exposure of the temporary secret keys at some periods will not enable an adversary to derive temporary secret keys for the remaining periods. Thus there is no need to change the public key, which is a desirable property for IBE systems. Hanaoka, Hanaoka, Shikata and Imai [22] applied the key-insulation mechanism to IBE system and proposed an ID-based hierarchical strongly key-insulated encryption scheme which is secure in the random oracle model.

Hanaoka et al. [20] first noticed the following situations in public key-insulated encryption (PKIE) schemes: when key-exposure occurs in key-insulated cryptosystems, to alleviate the damage, temporary secret key has to be updated at very short intervals; however, this will in turn increase the frequency of helper's connection to insecure environments and increase the risk of helper key-exposure. Keep in mind that once the helper key is exposed, the PKIE scheme will be broken if one of the temporary secret key is also exposed. Is it possible to