Information Sciences xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

ELSEVIER

UNCORRECTED PROOF

IRIBE: Intrusion-resilient identity-based encryption

Q1 Jia Yu[a,b,*], Rong Hao[a], Huawei Zhao[c], Minglei Shu[b], Jianxi Fan[d]

[a] *College of Information Engineering, Qingdao University, Qingdao 266071, China*
[b] *Shandong provincial Key Laboratory of Computer Network, Jinan 250014, China*
[c] *School of Computer and Information Engineering, Shandong University of Finance, Jinan 250014, China*
[d] *School of Computer Science and Technology, Soochow University, Suzhou 215006, China*

ARTICLE INFO

Article history:
Received 31 May 2014
Revised 12 May 2015
Accepted 14 September 2015
Available online xxx

Keywords:
Key exposure
Identity-based encryption
Forward security
Intrusion-resilient identity-based encryption
Standard model

ABSTRACT

In order to limit the damage of key exposure for identity-based encryption, we propose a new paradigm called intrusion-resilient identity-based encryption (IRIBE) in this paper. Compared with key-insulated identity-based encryption and forward-secure identity-based encryption, IRIBE can achieve a stronger level of security. In our proposed scheme, the ciphertexts in any other time periods are secure even after arbitrarily many compromises of the base and the user, as long as compromises do not happen simultaneously. Furthermore, the intruder cannot decrypt the ciphertexts pertaining to previous time periods, even if it compromises the base and the user simultaneously. Therefore, our IRIBE scheme can greatly enhance the security of identity-based encryption. We also formalize the definition and the security notions of this paradigm. The proposed scheme is proven secure in the standard model.

© 2015 Published by Elsevier Inc.

1. Introduction

The motivation of identity-based encryption introduced by Shamir [21] was to simplify key management process and eliminate the need for certificates. In an identity-based encryption scheme, the public key is replaced by any user's identity information while the associated secret key is generated by a trusted Private Key Generator (PKG). Identity-based encryption schemes have attracted much attention since the concept's appearance. Many schemes [2,3,7,11,15, 22,] about identity-based encryption have been proposed in the last decade.

Regular identity-based encryption crucially depends on the privacy of secret keys. However, it is very difficult to keep secret keys absolutely secure with more and more mobile and unprotected devices used in cryptographic primitives. It is indeed generally much easier for an adversary to obtain the user's secret key by breaking into the device than cracking actual cryptographic assumptions on which the system is based [26]. Once a secret decryption key is exposed, all the ciphertexts related to the corresponding public encryption key could be decrypted. We have to revoke the pair of secret decryption key and public encryption key, and issue a new pair. This problem seems especially serious for identity-based encryption because the public encryption key corresponding to the user's identity is not easy to change.

Key-evolving cryptosystems can reduce the threat of key exposure. In a key-evolving cryptosystem, the whole lifetime is divided into multiple time periods. Secret keys evolve in different time periods, while the public key is fixed. There are three kinds of key-evolving cryptosystems: forward-secure cryptosystem, key-insulated cryptosystem and intrusion-resilient cryptosystem. Forward-secure encryption [8] can protect the security of ciphertexts before key exposure, but cannot protect the security after

[*] Corresponding author. Tel.: +86 053285953151.
E-mail address: qduyujia@gmail.com (J. Yu).

http://dx.doi.org/10.1016/j.ins.2015.09.020
0020-0255/© 2015 Published by Elsevier Inc.

Please cite this article as: J. Yu et al., IRIBE: Intrusion-resilient identity-based encryption, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.09.020

UNCORRECTED PROOF

key exposure. Key-insulated encryption and intrusion-resilient encryption can keep the security not only before key exposure but also after key exposure, at the cost of introducing an entity (i.e. the base) to help the user update its secret keys. In key-insulated encryption [1,10,14,17,20], the user holds the secret decryption key, and can decrypt the ciphertexts on its own. At the end of each time period, the user would update its secret decryption key by communicating with the base and performing some local computations. As a result, the exposure of the user's current secret key does not compromise the security for the past periods and the future periods. However, the security will be wholly lost in key-insulated encryption when the user and the base are corrupted in the same period. Intrusion-resilient encryption [12,13,16] is as key-insulated encryption: the user decrypts the ciphertexts on its own with the secret key it holds, and the secret key update needs an update message from the base. Different from key-insulated encryption, intrusion-resilient encryption refreshes the secret keys of the user and the base many times in one period, which makes the intruder unable to get the secret keys of other periods even after arbitrarily many compromises of the user and the base, as long as these compromises do not happen simultaneously. Furthermore, the intruder cannot decrypt the ciphertexts pertaining to previous time periods, even if it compromises the user and the base simultaneously.

Forward-secure mechanism and key-insulated mechanism have been applied to identity-based encryption to deal with the key-exposure problem in [25,27] and [23,19,24], respectively. However, applying intrusion-resilient mechanism to identity-based encryption is still an unsolved problem up to now. Indeed, intrusion-resilient model appears to provide the maximum possible security in the face of key exposure. Therefore, intrusion-resilient mechanism can greatly enhance the security of identity-based encryption. How to make identity-based encryption with intrusion-resilient security is an important problem.

Seo et al. proposed a revocable identity-based encryption with decryption key exposure resilience [29]. In Seo's scheme, the adversary is allowed to obtain the decryption key $dk_{ID^*,t}$ $(t \neq t^*)$ for the challenged identity $ID^*(t^*$ is the challenged time period), which only provides partial secret key exposure resilience. Specifically, the secret key of the user with identity ID in [29,30] is composed by two parts. One part is the private key sk_{ID}, which is used to generate decryption key $dk_{ID,t}$. The other part is the decryption key $dk_{ID,t}$, which is used to decrypt the ciphertext. Seo's scheme can only deal with the decryption key $dk_{ID,t}$ exposure problem. If the full secret key (composed by sk_{ID} and $dk_{ID,t}$) is exposed, the security will completely lose. In practice, when the adversary compromises the user in time period t, he should get not only the decryption key $dk_{ID,t}$ but also the private key sk_{ID}. Therefore, Seo's scheme is not able to deal with the real key exposure in actual scenarios.

Q2

1.1. Our contribution

In order to resolve the above problem, we propose a new paradigm called intrusion-resilient identity-based encryption (IRIBE) in this paper. We firstly give the definition and the security notions of IRIBE scheme. And then construct the first IRIBE scheme. In our scheme, decryption keys evolve in regular intervals, while the identity information corresponding to the public key is unchanged during the whole lifetime. The ciphertexts in any other time periods are secure even after arbitrarily many compromises of the user and the base, as long as these compromises do not happen simultaneously. In addition, the intruder cannot decrypt the ciphertexts pertaining to previous time periods, even if it compromises the user and the base simultaneously. Intuitively, we make use of the hierarchical key derivation method in [3], which can be thought of as the binary tree encryption suggested by Canetti et al. [8]. In our scheme, Waters's identity-based encryption [22] is used at the lowest level of our hierarchical encryption. The message used to update keys is divided into two parts held by the base and the user, respectively. So the key update must be completed by the cooperation of the base and the user. The decryption secret key is only held by the user. As a result, the user can accomplish decryption operations himself. These designs can make our scheme achieve the intrusion-resilient security. Finally, we prove the proposed scheme is semantically secure in the standard model.

As the same as the standard key evolving cryptography [12,13,16,19,23,24,25,27], our scheme can solve the real key exposure problem, that is, our scheme allows the adversary to obtain the full secret key of the user. So the security of our scheme is higher than the security of Seo's scheme. In our scheme, the secret keys of the user and the base are refreshed many times in one period. As a result, the ciphertexts in any other time periods are secure even after arbitrarily many compromises of the base and the user, as long as compromises do not happen simultaneously. Furthermore, the adversary is even allowed to get all secret key information of the base and the user. The adversary cannot decrypt the ciphertexts pertaining to previous time periods, even if it compromises the base and the user simultaneously in our scheme. Different from Seo's scheme, our scheme does not consider the problem of identity revocation and the key update message is generated by the base. Because one base only serves for one or at most several users, our scheme does not need to consider the problem of scalability.

1.2. Organization

In the following section, we introduce the preliminaries of our work, including cryptographic assumption, the definition of intrusion-resilient identity-based encryption scheme and its security notions. A concrete description of our scheme is given in Section 3. In addition, Section 4 gives the security analysis of the scheme. Finally, we conclude the paper in Section 5.

2. Preliminaries

2.1. Cryptographic assumption

We firstly review some common cryptographic prelimilaries about bilinear maps and the decisional *l-wBDHI* assumption. Q3

Please cite this article as: J. Yu et al., IRIBE: Intrusion-resilient identity-based encryption, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.09.020

Download English Version:

https://daneshyari.com/en/article/6857423

Download Persian Version:

https://daneshyari.com/article/6857423

Daneshyari.com