Journal of Network and Computer Applications 34 (2011) 1724–1731

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

New identity-based key-insulated convertible multi-authenticated encryption scheme

Chien-Lung Hsu [a,b], Han-Yu Lin [c,*]

[a] Department of Information Management, Chang Gung University, Tao-Yuan, 333 Taiwan, ROC
[b] Taiwan Information Security Center at NTUST (TWISC@NTUST), Taipei 106, Taiwan, ROC
[c] Department of Information Management, Kainan University, Tao-Yuan, 338 Taiwan, ROC

ARTICLE INFO

Article history:
Received 15 November 2010
Received in revised form
26 April 2011
Accepted 12 June 2011
Available online 22 June 2011

Keywords:
Identity-based
Key-insulated
Convertible
Multi-authenticated encryption
Bilinear pairing

ABSTRACT

Elaborating on the merits of convertible multi-authenticated encryption (CMAE) schemes and key-insulated systems, we propose a novel identity-based key-insulated convertible multi-authenticated encryption scheme (IB-KI-CMAE), which can effectively reduce the impact caused by the key exposure. Our scheme allows each user to periodically update his private key while the corresponding public one remains unchanged. Additionally, a group of signers can cooperatively generate an authenticated ciphertext such that only the designated recipient has the ability to decrypt the ciphertext and verify their signature. In case of a later dispute over repudiation, the designated recipient can easily reveal the converted multi-signature for public arbitration. Our scheme can bring crucial benefits to the applications such as joint account and business contract signing. Moreover, in the random oracle model, we also formally prove that the proposed scheme achieves the security requirement of confidentiality against indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA).

1. Introduction

To deal with the public key substitution attack, in 1984, Shamir addressed the famous identity-based system in which the public key of each user is straightly his/her identifier information. A private key generation center (PKG) is responsible for generating all users' private keys, which will be sent to each user via a secure channel. Since the public key is explicitly verified, it is unnecessary to maintain a public key certificate. However, if a user's private key is accidentally compromised, it will cause the extra burden to reset the private key.

A key-insulated cryptosystem proposed by Dodis et al. (2002, 2003) can effectively mitigate the impact caused by the key exposure. In such a system, every user owns a short-term private key and a long-term one. The former is used for various cryptographic operations such as encryption and digital signature schemes (ElGamal, 1985; Rivest et al., 1978; Schnorr, 1991). The latter is stored in a physically secure but computation limited device (called base or helper). In different time periods, a user can periodically update his private key with the assistance of his helper. Even if an adversary successfully obtains the private key for the current time period, he cannot learn any information, which is protected by the private keys of previous time periods. Further considering the applications of pairing-based cryptosystems, in 2005, Hanaoka et al. introduced the first identity-based key-insulated encryption (IB-KIE) and its applications based on bilinear pairings. The next year, Zhou et al. (2006) presented an identity-based key-insulated signature (IB-KIS) scheme. In the random oracle model, they also formally proved the security of their scheme.

To eliminate the security vulnerability caused by the exposure of user's helper, Hanaoka et al. (2006) came up with a so-called parallel key-insulated encryption (KIE) scheme in which two independent helpers are adopted. Each time when a user attempts to update his private key, he can choose either of the helpers to assist with the updating process, so as to increase the security of helpers. To give more flexibility of use, in 2008, Weng et al. proposed an identity-based (k, n) threshold KIE scheme using n helpers. In their system, at least k helpers are sufficient to perform the key-update procedure while less than or equal to $k-1$ cannot. In 2010, Yu et al. proposed an IB-KIS scheme providing not only efficient key-update procedure, but also provable security in the random oracle model. Their scheme has crucial benefits to the practical applications like full delegation proxy signature scheme with time restriction.

To provide the digital signature scheme with the property of confidentiality (Delfs and Knebl, 2002), in 1994, Horster et al.

* Corresponding author. Tel.: +886 926 377200.
E-mail address: hanyu.cs94g@nctu.edu.tw (H.-Y. Lin).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.06.005