ID-BASED KEY-INSULATED SIGNATURE SCHEME WITH BATCH VERIFICATIONS AND ITS NOVEL APPLICATION

Tsu-Yang Wu, Yuh-Min Tseng* and Ching-Wen Yu
Department of Mathematics
National Changhua University of Education
Jin-De Campus, No. 1, Jin-De Road, Chang-Hua 500, Taiwan
*Corresponding author: ymtseng@cc.ncue.edu.tw
Received March 2011; revised September 2011

Abstract. For a digital signature scheme, loss of private keys will cause a devastating effect on e-commerce and Internet-based transaction applications in the present network environment. Key-insulated public-key system is introduced to reduce damage caused by private key exposure. Over the last few years, identity (ID)-based key-insulated cryptography using bilinear pairings has received much attention from cryptographic researchers. In this paper, we propose a new and efficient ID-based key-insulated signature scheme with batch verifications. As compared with the recently proposed ID-based key-insulated signature schemes, our scheme has the best performance for batch verifications. For security analysis, we demonstrate that the proposed scheme is a provably secure ID-based key-insulated signature in the random oracle model and under the computational Diffie-Hellman assumption. Meanwhile, to demonstrate the additional advantage of our ID-based key-insulated signature scheme, we present a novel application based on the proposed scheme, called ID-based proxy signature scheme with full delegation and time restriction. This new type of proxy signature scheme provides flexible management for the delegated proxy signers.

Keywords: Key-insulated, Signature, Batch verification, ID-based, Proxy signature

1. Introduction. Exposure of private keys in cryptographic mechanisms (e.g., digital signature and cryptosystem) is the greatest harm to users and means that all security goals are entirely lost. In 2002, Dodis et al. introduced the first key-insulated public-key system [8,9] to solve the problem of regarding cryptographic system injury caused by user’s private key exposure. In their key-insulated public-key system, the private keys at discrete various time periods are different and could be stored on an insecure device. Each user must periodically refresh her/his private key through a physically-secure device, named a helper, and the user’s public key remains unchanged and fixed throughout the lifetime of the key-insulated public-key system. If an adversary revealed a user’s present private key, the adversary is still unable to compute the user’s former or later private keys. Hence, the key-insulated public-key system can be used to reduce damage caused by private key exposure.

In 1984, Shamir [18] proposed the first identity (ID)-based public-key cryptosystem. In an ID-based public key system, a user’s public key is determined by his/her identity (e.g., name, e-mail address, or social security number). As compared with the traditional certificate-based public-key systems, ID-based public-key system may simplify certificate management. However, Shamir’s system is not easy to be realized in practice. In 2001, Boneh and Franklin [3] proposed a practical ID-based cryptosystem from the Weil pairing defined on elliptic curves. Later on, many ID-based cryptographic schemes and protocols from bilinear pairings were proposed in [4,6,7,25,26].