2009 International Conference on Availability,
Reliability and Security (ARES2009), Japan: 935-940

Towards Efficient ID-based Signature Schemes with Batch Verifications from Bilinear Pairings

Tseng, Yuh-Min; Wu, Tsu-Yang; Wu, Jui-Di

Abstract

Many group-oriented applications and multicast communications often need to verify which group members have sent/received a message. However, individual verification of signed messages would require a significant computation cost. A secure signature scheme with supporting variant batch verifications extremely improves performance. In 2003, Cha and Cheon proposed an efficient identity (ID)-based signature scheme with bilinear pairings. Recently, Yoon et al. pointed out that their scheme does not provide batch verifications for multiple signatures. In this paper, we examine and discuss twelve kinds of Cha-Cheon like signature schemes and security properties. We obtain an efficient ID-based signature scheme supporting batch verifications. In the random oracle model and under the computational Diffie-Hellman assumption, we show that this new scheme is secure against existential forgery attacks under various types of batch verifications.