IEICE Transactions on Fundamentals of Electronics,
Communications and Computer Sciences, E92-A(10): 2638-2640

Comments on an ID-Based Authenticated Group Key Agreement Protocol with Withstanding Insider Attacks

Wu, Tsu-Yang; Tseng, Yuh-Min

Abstract

In PKC 2004, Choi et al. proposed an ID-based authenticated group key agreement (AGKA) protocol using bilinear pairings. Unfortunately, their protocol suffered from an impersonation attack and an insider colluding attack. In 2008, Choi et al. presented an improvement to resist insider attacks. In their modified protocol, they used an ID-based signature scheme on transcripts for binding them in a session to prevent replay of transcripts. In particular, they smartly used the batch verification technique to reduce the computational cost. In this paper, we first show that Choi et al.'s modified AGKA protocol still suffers from an insider colluding attack. Then, we prove that the batch verification of the adopted ID-based signature scheme in their modified protocol suffers from a forgery attack.

Key words：Group key agreement; Insider colluding attack; Batch verification; Forgery attack