Jordan University of Science and Technology

Id-Based Mutual Authentication with Signcryption Scheme for Mobile Devices

Authors: Bushra Al-Ja'afreh, Mohammad Alhammouri, and Qusai Abuein

Abstract: Signcryption is a cryptographic primitive technique that combines digital signature and public key encryption in one logical single step. Signcryption scheme is divided into certificate-based Signcryption scheme, and certificateless Signcryption scheme. In this paper we propose an identity based mutual authentication protocol that provides signed and encrypted communication based on Signcryption scheme between mobile devices that are limited in terms of computation power. The proposed protocol is based on Certificateless Signcryption, in which no Digital Certificate Authorities are used to manage user identities, their public keys, and certificate lifecycle. Our proposed protocol allows limited computation power devices to delegate identity validation that requires lots of computation and cryptographic operations to a third party. Our proposed scheme depends on (ECC) which has efficient delivery of security services and is better than exponential cryptography. Our proposed scheme also provides several security services such as, confidentiality, mutual authentication, integrity, unforgeability, non-repudiation, public verifiability and perfect forward secrecy.