World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:01, 2015

Efficient Signcryption Scheme with Provable Security for Smart Card

Authors : Jayaprakash Kar, Daniyal M. Alghazzawi

Abstract : The article proposes a novel construction of signcryption scheme with provable security which is most suited to implement on smart card. It is secure in random oracle model and the security relies on Decisional Bilinear Diffie-Hellmann Problem. The proposed scheme is secure against adaptive chosen ciphertext attack (indistiguishbility) and adaptive chosen message attack (unforgebility). Also, it is inspired by zero-knowledge proof. The two most important security goals for smart card are Confidentiality and authenticity. These functions are performed in one logical step in low computational cost.

Keywords : random oracle, provable security, unforgebility, smart card
Conference Title : ICSC 2015 : International Conference on Security and Cryptography
Conference Location : Jeddah, Saudi Arabia
Conference Dates : January 26-27, 2015