World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:9, No:07, 2015

Cryptanalysis of ID-Based Deniable Authentication Protocol Based On Diffie-Hellman Problem on Elliptic Curve

Authors : Eun-Jun Yoon

Abstract : Deniable authentication protocol is a new security authentication mechanism which can enable a receiver to identify the true source of a given message, but not to prove the identity of the sender to a third party. In 2013, Kar proposed a secure ID-based deniable authentication protocol whose security is based on computational infeasibility of solving Elliptic Curve Diffie-Hellman Problem (ECDHP). Kar claimed that the proposed protocol achieves properties of deniable authentication, mutual authentication, and message confidentiality. However, this paper points out that Kar's protocol still suffers from sender spoofing attack and message modification attack unlike its claims.

Keywords : deniable authentication, elliptic curve cryptography, Diffie-Hellman problem, cryptanalysis
Conference Title : ICPECCS 2015 : International Conference on Pervasive, Embedded Computing and Communication Systems
Conference Location : Prague, Czechia
Conference Dates : July 09-10, 2015