World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:07, 2016

An Efficient Proxy Signature Scheme Over a Secure Communications Network

Authors : H. El-Kamchouchi, Heba Gaber, Fatma Ahmed, Dalia H. El-Kamchouchi

Abstract : Proxy signature scheme permits an original signer to delegate his/her signing capability to a proxy signer, and then the proxy signer generates a signing message on behalf of the original signer. The two parties must be able to authenticate one another and agree on a secret encryption key, in order to communicate securely over an unreliable public network. Authenticated key agreement protocols have an important role in building secure communications network between the two parties. In this paper, we present a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on the discrete logarithm problem.

Keywords : proxy signature, warrant partial delegation, key agreement, discrete logarithm
Conference Title : ICCSCS 2016 : International Conference on Cryptography and Security in Computing Systems
Conference Location : Zurich, Switzerland
Conference Dates : July 21-22, 2016