World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:06, 2016

A Secure Proxy Signature Scheme with Fault Tolerance Based on RSA System

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

Abstract : Due to the rapid growth in modern communication systems, fault tolerance and data security are two important issues in a secure transaction. During the transmission of data between the sender and receiver, errors may occur frequently. Therefore, the sender must re-transmit the data to the receiver in order to correct these errors, which makes the system very feeble. To improve the scalability of the scheme, we present a secure proxy signature scheme with fault tolerance over an efficient and secure authenticated key agreement protocol based on RSA system. Authenticated key agreement protocols have an important role in building a secure communications network between the two parties.

Keywords : proxy signature, fault tolerance, rsa, key agreement protocol
Conference Title : ICCCS 2016 : International Conference on Cryptology and Computer Security
Conference Location : Copenhagen, Denmark
Conference Dates : June 27-28, 2016