World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:09, 2016

A Secure Digital Signature Scheme with Fault Tolerance Based on the Improved RSA System

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

Abstract : Fault tolerance and data security are two important issues in modern communication systems. In this paper, we propose a secure and efficient digital signature scheme with fault tolerance based on the improved RSA system. The proposed scheme for the RSA cryptosystem contains three prime numbers and overcome several attacks possible on RSA. By using the Chinese Reminder Theorem (CRT) the proposed scheme has a speed improvement on the RSA decryption side and it provides high security also.

Keywords : digital signature, fault tolerance, RSA, security analysis
Conference Title : ICFCDS 2016 : International Conference on Financial Cryptography and Data Security
Conference Location : Rome, Italy
Conference Dates : September 15-16, 2016