World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:07, 2014

# Using the Cluster Computing to Improve the Computational Speed of the Modular Exponentiation in RSA Cryptography System

**Authors :** Te-Jen Chang, Ping-Sheng Huang, Shan-Ten Cheng, Chih-Lin Lin, I-Hui Pan, Tsung- Hsien Lin

**Abstract :** RSA system is a great contribution for the encryption and the decryption. It is based on the modular exponentiation. We call this system as “a large of numbers for calculation”. The operation of a large of numbers is a very heavy burden for CPU. For increasing the computational speed, in addition to improve these algorithms, such as the binary method, the sliding window method, the addition chain method, and so on, the cluster computer can be used to advance computational speed. The cluster system is composed of the computers which are installed the MPICH2 in laboratory. The parallel procedures of the modular exponentiation can be processed by combining the sliding window method with the addition chain method. It will significantly reduce the computational time of the modular exponentiation whose digits are more than 512 bits and even more than 1024 bits.

**Keywords :** cluster system, modular exponentiation, sliding window, addition chain
**Conference Title :** ICISET 2014 : International Conference on Information Science, Engineering and Technology
**Conference Location :** Singapore, Singapore
**Conference Dates :** July 05-06, 2014