Abstract

Numerous decryption and encryption algorithmic methods have been proposed and applied in prior research, including RSA, DES, etc. Such methods are normally assessed in their performance in accordance with the growth rates of their algorithms, based on key and input sizes. With RSA public-key security algorithms, primary operations feature modular exponentiations and reductions. As a result, sequential implementations of RSA become more computing-time, and energy-intensive. Several parallelization methods are therefore recommended in order to improve the speed of RSA algorithms. In this paper, parallel RSA algorithmic methods are assessed and then compared, based on decryption and encryption running times, speedup, and efficiency. The experimental results show that the runtime of parallel RSA algorithmic method outperform those of sequential RSA algorithmic methods.

References

Performance of Parallel RSA on IMAN1 Supercomputer

cryptography. CRC press.


Index Terms

Computer Science  Algorithms

Keywords

Cryptography, RSA, MPI, Supercomputer, Public Key, Private Key, Parallel algorithm