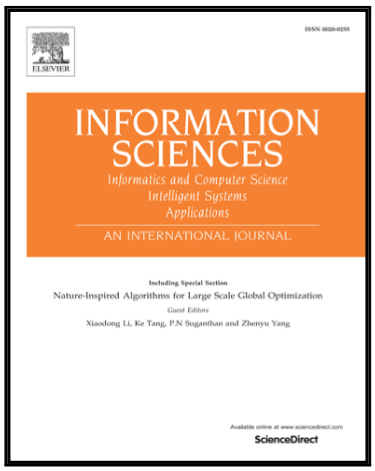

Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing

Laurence T. Yang, Gaoyuan Huang, Jun Feng, Li Xu

PII: S0020-0255(16)31234-8
DOI: 10.1016/j.ins.2016.10.017
Reference: INS 12576

To appear in: *Information Sciences*

Received date: 31 January 2016
Revised date: 1 October 2016
Accepted date: 9 October 2016

Please cite this article as: Laurence T. Yang, Gaoyuan Huang, Jun Feng, Li Xu, Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.10.017

Parallel GNFS Algorithm Integrated with Parallel Block Wiedemann Algorithm for RSA Security in Cloud Computing

Laurence T. Yang[a], Gaoyuan Huang[a], Jun Feng[b], Li Xu[a]

[a]*Department of Mathematics, Statistics and Computer Science, St. Francis Xavier University, Antigonish, NS, Canada*
[b]*School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China*

Email: ltyang@gmail.com

Abstract

RSA algorithm is one of the most popular and secure public key cryptographic algorithms. To guarantee data security in cloud computing, RSA algorithm has been widely used in cloud. The security of RSA algorithm lies in the difficulty of factoring large integers efficiently. The General Number Field Sieve (GNFS) algorithm is the most efficient algorithm for factoring integers greater than 110 digits at present, and cloud computing is able to provide powerful ability for carrying out GNFS algorithm. Focussing on the research regarding security of RSA, in this paper, we study the GNFS algorithm in cloud. More specifically, we discuss the current research about solving large and sparse linear systems over GF(2), which is one of the most time-consuming steps of the GNFS algorithm. Then, we propose a novel parallel block Wiedemann algorithm in cloud to reduce the communication cost of solving large and sparse linear systems over GF(2). The proposed parallel block Wiedemann algorithm includes strip partitioning, cyclic partitioning, and improved strip partitioning which accelerate different steps in the block Wiedemann algorithm in a parallel way. Theoretical and experimental results show that the parallel block Wiedemann algorithm can greatly enhance the performance of GNFS compared with other existing algorithm, in terms of both execution time and speedup.

Keywords: Cloud computing; RSA; Security; GNFS; Block Wiedemann;