Department of Mathematics, Statistics and Computer Science
St. Francis Xavier University
Presents

Wiedemann-based Parallel GNFS Algorithms for Integer Factorization

by
Alan Gaoyuan Huang
St. Francis Xavier University
MSc Student

Monday, January 12th, 2009 @ 2:45 in AX23A

RSA is one of the most popular public-key cryptographic algorithms at present. The strength of RSA algorithm lies on the difficulty of factoring large integers efficiently. GNFS algorithm is currently the most efficient algorithm for factoring integers greater than 110 digits. One of the most time consuming steps in GNFS algorithm is solving large sparse linear systems over GF(2). In the thesis, the Wiedemann algorithm and its block version have been adapted and paralleled in order to speed up the step of solving large sparse linear systems over GF(2) in GNFS algorithm. Some preliminary experimental results conducted on high performance computer architectures will be presented and the plan for future work will also be described.

Refreshments will be served before the talk in AX24A