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

An Improved Parallel Block Lanczos Algorithm over GF(2) for Integer Factorization

by

Alice Ying Huang

MSc Student

St. Francis Xavier University

Friday, December 4th, 2009 @ 1:15 in Ax23A

RSA is one of the most popular algorithms for public-key cryptosystems**.** The security of this algorithm relies on the difficulty of factoring large integers. GNFS is the most efficient algorithm for factoring large integers over 110 digits, and solving the large sparse linear system over GF(2) is one of the most time-consuming steps in the GNFS. In the thesis proposal, an improved and more efficient parallel Block Lanczos algorithm for large and sparse linear systems over GF(2) has been proposed. In order to greatly improve the performance over distributed memory parallel computer architectures, the original algorithm has been re-organized and re-designed in order to reduce the synchronization as much as possible, while data distribution has been carefully studied as well, both to minimize the communication costs among parallel processors. Further comprehensive analyses and experimental results will be investigated and conducted in the future MSc study.

Refreshments will be served before the talk in AX24A