ST. FRANCIS XAVIER UNIVERSITY

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

Scalable GNFS Algorithm for Integer Factorization

by

Sazzad Hussain

St. Francis Xavier University

M.Sc. Thesis Proposal Presentation

April 23 2018 @ 10:15am in Annex 23A

The RSA algorithm is one of the most popular and secure public key cryptographic algorithms. It has been widely used in many real-life applications because of its simplicity and ease of implementation. The security of the RSA algorithm lies in the difficulty of factoring large integers efficiently, that is, if the large integers can be factored in a reasonable time, then the RSA cryptosystem is no longer secure. At present, the General Number Field Sieve (GNFS) algorithm is the most efficient algorithm for factoring integers greater than 110 digits. The most recent well-known efficient implementation of GNFS algorithm for integer factorization is CADO-NFS. There are five major parts in this implementation. In this thesis, we have studied and analyzed every part of it, but mainly focus on Linear algebra step which is one of the most time-consuming parts of GNFS algorithm. We have also studied some most efficient techniques in solving large and sparse linear system over GF(2). Based on these, we propose a more scalable and efficient implementation to be integrated into CADO-NFS especially for high performance computer architectures. Comprehensive test cases and experimental results will be conducted to demonstrate the superior performance of our proposed approach.