Two Elliptic Curve Method Factoring Programs

Major Professor: **Samuel S. Wagstaff, Jr.**
Researcher: **Abhilasha Bhargav**

The Abstract:

The Elliptic Curve Method (ECM) is used to factor numbers of the form 2^N-1 and 2^N+1 . There are several prizes for factoring Fermat numbers, or gain a small footnote in math history by finding a new factor for the Cunningham tables, or improve Paul Leyland's table for Mersenne numbers below 10,000, etc.

My aim in the project is first to download two ecm programs, with the respective libraries, then run and debug them in a sun work station. This is the improved version from Paul Zimmermann (Inria), and on comparing it with what is known, I should get similar results with the run times also close to the value known.

Once this is done, another file will be downloaded which is made to run faster on the sun machine whereas the former was optimized for PC's and Alpha's. This new file uses MAGMA (Computer Algebra Package, which is useful to researchers in Cryptography).

After these two (C) programs are working successfully, I will port them into an IBM SP and see which one is faster there, running on just one processor. Next, the faster one is taken and made parallel by running it with more than one processor.

This would accomplish more calculations in lesser time, and the probability of a number getting factorized would be increased.