DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

Implementation of the Hypercube Variation of the Multiple Polynomial Quadratic Sieve

René Peralta
Electrical Engineering and Computer Science Department
University of Wisconsin at Milwaukee

Tuesday, May 16, 1995, at 2:15 PM
The Seminar Room

Abstract: We discuss the implementation of the Hypercube variation of the Multiple Polynomial Quadratic Sieve (HMPQS) integer factorization algorithm. HMPQS is a variation on Pomerance's Quadratic Sieve algorithm which inspects many quadratic polynomials looking for quadratic residues with small prime factors. The polynomials are organized as the nodes of an n-dimensional cube. Since changing polynomials on the hypercube is cheap, the optimal value for the size of the sieving interval is much smaller than in other implementations of the Multiple Polynomial Quadratic Sieve (MPQS). This makes HMPQS substantially faster than MPQS. We also describe a relatively fast way to find good parameters for the single large prime variation of the algorithm. Finally, we report on the performance of our implementation on factoring several large numbers for the Cunningham Project.

Joan F. Boyar