AN UPDATE ON FACTORIZATION AT SANDIA NATIONAL LABORATORIES*

J. A. Davis and D. B. Holdridge

Sandia National Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

Since Crypto 83 we have had considerably more experience in factoring large integers. Implementation of various modifications to the quadratic sieve algorith have enabled the factorization of hard 70-digit numbers in times comparable to 50 digits one year ago. These modifications include:

1) Subsequences with large divisors (Special q's).
2) Multipliers to improve quadratic properties.
3) Increased size of prime base using segmented Gaussian Elimination.
4) Optimization of the code with respect to Cray hardware.

Using this code in its various stages of development the 10 most wanted numbers from the Cunningham Project have been factored. Details will be published elsewhere.

* This work was performed at Sandia National Laboratories supported by the U. S. Department of Energy under Contract No. DE-AC04-76DP00789.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, p. 114, 1985.
© Springer-Verlag Berlin Heidelberg 1985