

1077-11-881

David Harvey*, School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia. *Faster deterministic integer factorization.*

The best known deterministic complexity bound for computing the prime factorization of an integer n is $O(M(n^{1/4} \log n))$, where $M(k)$ denotes the cost of multiplying k -bit integers. This result is due to Bostan–Gaudry–Schost, following the Pollard–Strassen approach. We show that this bound can be improved by a factor of $\sqrt{\log \log n}$. This is joint work with Edgar Costa (New York University). (Received September 13, 2011)