The PRIMES Challenge

The problem to decide whether a given integer n is prime or composite has a long history. In a very recent preprint (August 6, 2002), Agrawal, Kayal, and Saxena of IIT Kanpur present a deterministic polynomial time algorithm for this problem, see `http://www.cse.iitk.ac.in/primality.pdf`. The algorithm seems to be correct. However, the complexity of the algorithm is $O((\log n)^{12} poly(\log \log n))$.

Challenge I offer an award of US \$100 for the first person to find a deterministic algorithm for PRIMES with at most $O((\log n)^3 poly(\log \log n))$ time complexity.

Hint Prove the conjecture stated in the paper.

Restriction You need to be affiliated with Texas A&M University to be eligible for this award.

Background R. Crandall, C. Pomerance: Prime Numbers, Springer 2001.

Good luck!

Andreas Klappenecker
Department of Computer Science
Texas A&M University
Office: HRBB 509B