

Re: Interesting Factoring Paper

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00489.html>

- *From:* mm <mm@xxxxxxxxxx>
 - *Date:* Sat, 15 Jul 2006 02:34:50 +0200
-

Tom St Denis a écrit :

OMG Surrogate FACTORING!!!

Kidding. Here's a quick paper on AKS.

<http://eprint.iacr.org/2006/232>

I don't know if this paper is correct (it surely is) but I regret that the author doesn't give an estimate of the time needed to certify the 500-digit number he quotes at the end.

He concludes with

"Hence to show that n is prime it is sufficient to show the following:"

and, among the "following",

"that equalities $(x-b)^n = x^n - b \pmod{(n, x^r - 1)}$ hold for all 74023 elements of the set S_1 ."

Observe that $x^r - 1$ is a polynomial of degree 2,755,759.

For the sake of comparison, the certification of n with ECPP took 63s (AMD 3200+) [*]. As a bonus, with ECPP, you got a certificate that can be checked in less than 5s and whose non-validity would prove there was a problem during the certification (n is composite, bug, loss of bits, etc).

[*] 32-bit version

mm

.