

Re: SF: Back to theory

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4501.html>

jstevh_at_msn.com

Date: 02/25/05

Date: 24 Feb 2005 19:35:44 -0800

jst...@msn.com wrote:

- > *I see a lot of negative postings about my ideas, and surrogate*
- > *factoring is getting a lot of bashing, but hey, it's just an idea.*
- >
- > *It may not be practical--ever. But it's still just an idea, and I*
- > *can*
- > *discuss it as just an idea, having long ago backed away from calling*
- > *it*
- > *a solution to the factoring problem.*
- >
- > *Now some posters seem to be obsessed with political posting meant to*
- > *drive others away from my idea. I say, look at what they're doing as*
- > *just that--political postings.*
- >
- > *Now to the theory.*
- >
- > *Basically with the latest surrogate factoring I've been analyzing the*
- > *quadratics:*
- >
- > $yx^2 + Ax - M^2 = 0$
- >
- > *and*
- >
- > $yz^2 + Az - j^2 = 0$
- >
- > *where $T = M^2 - j^2$*
- >
- > *and my algorithms focus on y, for several reasons, not the least of*
- > *which it *seems* to only need the factorization of T, while other*
- > *algorithms, which I'll get to later, require that both j and T be*
- > *factored, while doing far worse than algorithms that just use*
- > *factoring T.*
- >
- > *Now an easy thing to do is just subtract the first equation from the*
- > *second:*
- >
- > $y(x^2 - z^2) + A(x-z) - M^2 + j^2 = 0,$
- >

> and, of course, $M^2 - j^2 = T$, so
>
> $y(x^2 - z^2) + A(x-z) - T = 0$,
>
> $y(x^2 - z^2) = T - A(x-z)$
>
> which gives that
>
> $y = (T + A(z-x))/(x^2 - z^2)$
>
> so I can kind of look at y, to the extent that you can tell anything
> from that equation.

I think it indicates there are blocking primes.

Blocking primes are primes forced in by the two squares in the denominator that are not factors of T, like if the numerators and denominators of x and z are coprime to 3, then the denominator is forced to have 3 as a factor, so 3 is a potentially blocking prime.

If all the blocking primes can be found, then they can each be handled, but I'm not exactly sure about whether or not my idea about blocking primes is correct.

I *have* forced factors of 3 into T, and the algorithm I have still doesn't *always* factor.

James Harris