

Re: SF: Back to theory

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/4505.html>

From: Nora Baron (norabaron_at_hotmail.com)

Date: 02/25/05

Date: 24 Feb 2005 19:48:26 -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.
>
> One thing that is clear is that the denominator of y for rational y's
> must be a perfect square, which you can see easily enough by solving
> for x with the first quadratic to get
>
> $x = (-A \pm \sqrt{A^2 + 4My})/2y$
>
> and that is visible by inspection.
>
> Notice also I can go back to my solution for y, and divide both sides
> by A^2 to get
>
> $y/A^2 = (T + A(z-x))/((Ax)^2 - (Az)^2)$
>
> where the equations again show a lack of dependency on the value of
> A,
> as it can be wrapped up into other expressions, which is a feature
> shown again when y is solved out, so that you have
>
> $Ax = Az(-Az \pm \sqrt{(Az - 2M^2)^2 - 4TM^2})/(2j^2 - 2Az)$
>
> and
>
> $Az = Ax(-Ax \pm \sqrt{(Ax - 2j^2)^2 + 4Tj^2})/(2M^2 - 2Ax)$
>
> which also shows that an integer Az must exist, with a rational Ax,
> that factors M.
>
> The problem has been figuring out how to find that integer Az or
> rational Ax, as it's *easy* to get integer Ax, but from postings on
> the
> sci.crypt newsgroup from people who claim to have tried it, it
> doesn't
> seem to factor all that often.
>
> But you can see two things, that a solution must exist, and that A
> can
> be wrapped up into x and z, such that its value need not be

determined.

>

> *Looking again at*

>

> $y/A^2 = (T + (Az - Ax))/((Ax)^2 - (Az)^2)$

>

> *you can see an assumption I'm making in my algorithms, where I*

> *basically assume that after common factors between*

>

> $((Ax)^2 - (Az)^2)$

>

> *and*

>

> $(T + (Az - Ax))$

>

> *are divided off, what remains only shares prime factors with T.*

>

> *Now that is the assumption I make in my algorithms, and it comes from*

a

> *solution I have for y, where I've related it to its own factor, and*

the

> *equation I solve to get that solution is*

>

> $f_1^2 s_1^4 - (A^2 + 4j^2 y + 2Ty)s_1^2 + f_2^2 y^2 = 0$

>

> *where $f_1 f_2 = T$, and $s_1 s_2 = y$ (the equation for s_2 differs only*

> *by indices),*

>

> *so I can look at how y is related to its own factor, and notice that*

> *the far left term has f_1^2 as a coefficient.*

>

> *With no other factors visible, it seems reasonable to suppose that*

the

> *denominator of y has prime factors of T only, but algorithms based on*

> *that idea do not always factor, and I don't know why.*

>

> *Now if you wish to derive that equation relating y to its own factor,*

> *it's not hard to do, but I'd just as soon refer you to the paper that*

> *steps through it, rather than make this post overly complicated.*

>

> *One thing worth mentioning is that explicit equations relating x and*

y

> *to factors of T and j are easily derived:*

>

> $y = A^2(f_1 - b_1)(f_2 - b_2)/(b_1 f_2 + b_2 f_1 - 2b_1 b_2)^2$

>

> *where $b_1 b_2 = -j^2$ and $f_1 f_2 = T$,*

>

> *and*

>

> $x = (b_1 f_2 + b_2 f_1 - 2b_1 b_2)/A.$

- >
- > *With all the detail available, it's of some interest that the complete*
- > *solution to the prime factors that make up the denominator of y seems*
- > *to be a hard problem, as with that solution, surrogate factoring can*
- be
- > *made to work perfectly.*
- >
- > *I still can't see why T doesn't provide all of those factors, given*
- the
- > *equation relating y to its own factor, but there must be some reason,*
- > *or the algorithms I've tried so far would work.*
- >

You have made this so much more complicated than it needs to be. Here is a simpler approach that may accomplish much the same and it is also much more general.

Assume M is the number to be factored. Pick a (small) integer j. Let $T = M - j$. Thus T is a function of both M and j.

Factor T. Assume you have split it into two factors, f and g. Thus $T = f * g$.

Now let X be some rational function of f and g. One possible choice might be,

$$X = (f - g) / (f + g).$$

Finally, let $Y = M / X$. Thus $M = X * Y$.

Note that X and Y are both functions of the factors of T. Also both are rational numbers. There is some chance that the numerator of X has a factor in common with M.

This is, certainly, surrogate factoring. Really, your underlying idea is not that different. What you are doing essentially is finding a more complex function to define X as a function of f and g.

Here is how this might work with $M = 15$. Let $j = 1$. Then $T = M - j = 14$. You factor T as $f * g = 7 * 2$. Then you note that

$$X = (7 - 2) / (7 + 2) = 5/9.$$

Right there, in the numerator, you have a factor that divides M.

Interestingly, the denominator, 9, also has a factor in common with M.

Let's try it on a bigger number. Say $M = 77$. This time let $j = 2$. $T = 75 = 3 * 5 * 5$. Let $f = 25$ and $g = 3$. Then

$$X = (f - g)/(f + g) = (25 - 3)/(25 + 3) = 22/28 = 11/14.$$

Note that the numerator of X, namely 11, is a factor of 77. And again, the denominator, 14, also has a factor in common with 77.

Pretty amazing, eh?

I am a little surprised myself. I typed out this whole message in the last 15 minutes. I just made up the function that defines X, $X = (f - g)/(f + g)$. I could have chosen an infinity of other functions. Also, quite honestly, I just made up the two examples. I must confess that I did try $j = 1$ with the second example mentally, and saw it was not going to work, so I tried $j = 2$. No other trial-and-error.

What's the point?

The point is, I have modified and greatly simplified your central idea – and at the same time, greatly generalized it – and on these two simple little examples – the only ones I have tried – it works. It might work on lots of other examples. If it doesn't, I can try changing the function that defines X. I can add parameters, like your A, y, and z. Your central theme, surrogate factoring of the number $T = M - j$, is still there, and it might even explain why it works (if it does). After all, the factors of M ought to be related somehow to the factors of T. In the case of RSA numbers, in general you expect T to be easier to factor than M.

Nora B.

> *All of this may be of "pure math" interest only, if these equations*
> *can't be turned into practical algorithms.*
>
>
> *James Harris*