

Re: Surrogate factoring, update

Source: <http://sci.tech--archive.net/Archive/sci.math/2004-07/2625.html>

From: James Harris (jstevh_at_msn.com)

Date: 07/11/04

Date: 11 Jul 2004 13:25:42 -0700

Matthijs Hebly <heeb@iname.com> wrote in message
news:<9B8Ic.114654\$3N6.81661@amsnews05.chello.com>...

> James Harris wrote:

> > Matthijs Hebly <heeb@iname.com> wrote in message
news:<hXUHc.98963\$3N6.21454@amsnews05.chello.com>...

> > > James Harris wrote:

> > > > It's been a while since I mentioned surrogate factoring, and I'll

> > > <znib>

> > > Maybe you should put your method to the test? Let your PC make a huge

> > <znib>

> > Theoretical work can be VERY trying to many people. They want to see

> > THE RESULT and have most of the details nailed down and have

> > CERTAINTY.

>

> It can be trying to mathematicians too. Was it just a waste of time when

> Naom Elkies found out that:

> $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$?

> No, because then people could stop looking for a proof that

> $x^4 + y^4 + z^4 = t^4$ doesn't have solutions for positive integers x, y, z, t ,

> because this idea obviously turned out to be false.

I don't disagree.

> Then there's the fact that you're posting in sci.crypt, and not only in

> sci.math. In sci.crypt, people are very much interested in *practical*

> as well as theoretical work. Questions like "How much faster is your

> method", "Can you give us some practical examples", etc., are as

> important here as the theory. It's nice to know a certain new method to

> accomplish something takes a time a factor 10^{200} less than an old

> method, but if this new method still takes $10^{(10^{38374646})}$ years given

> today's hardware, then it's nice to know but of no practical value to

> cryptography. So I repeat: if there's anything in your method (assuming

> you have one, which I cannot tell), then (at least in sci.crypt) give us

> an example of you factoring a huge composite using your method.

>

I don't know if its practical.

But if it is practical or can be made practical then it probably affects public key encryption.

It's scary because **theoretically** you can just factor some really big number like $T^2 - 1$ and use its factors to then factor T .

> > *However, no matter how certain so much knowledge that is tossed about*
> > *today is today, way back there were people at the beginning who were*
> > *lost and looking, trying to figure out what was going on.*
> *They were amazed that e.g. $3^2 + 4^2 = 5^2$. People have been playing*
> *with numbers always. So why don't you want to do this with your method?*
> *Come on James, give us an example!*
>

No matter how many of you are certain that sci.crypt is just about practical issues as if theory doesn't matter, I think there are others who think that cryptology cares about theoretical approaches as well as ones proven by demonstration.

My aim here is to discuss an idea that **might** have huge implications, and it might just be interesting, or it might not lead to much at all.

> > *From small beginnings come human civilization itself.*
> *Then give us a small beginning of an example. Break RSA a **little**.*
> *Slightly factor a composite that's just a **little** huge. After that the*
> *rest of us will tell you whether you'll have reached human civilization or*
> *not.*
>
> > *Here and now though, there's this idea I'm tossing around, and it's at*
> > *the beginnings. Will it be a super idea, a potent idea? I'm not certain,*
> > *though I definitely think it's worth discussing.*
> *Break RSA. Then you'll have your discussion I'm sure.*
>

If I knew I could definitely break RSA then I wouldn't be discussing this idea here.

> > *Now I know for some of you that's not the answer you want. You want*
> > *certainty. You want things nailed down and a fully fleshed out*
> > *product or theory.*
> *Isn't that why mathematicians are looking for proofs? They e.g. wanted*
> *certainty too that $x^n + y^n = z^n$ wouldn't have solutions for positive*
> *integers x, y, z, n with $n > 2$.*
>
> > *Most ideas don't pass all the tests.*
> *I guess here in sci.crypt people are interested in practical tests,*
> *because cryptography has practical as well as theoretical aspects.*
>
> *Matthijs Healy.*

You may guess all you wish, but you can't speak for everyone.

sci.math: Re: Surrogate factoring, update

The practical people can just wait and see or dismiss, while those who can get pulled in by theory can get involved.

I KNOW that for many of you it can be frustrating to hear about an idea when you want a product.

But that's basic research. It's why some people can do it, and most can't.

They can't handle the frustration and uncertainty.

James Harris