

Re: Gist of surrogate factoring theorem

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/0616.html>

jstevh_at_msn.com

Date: 04/10/05

Date: 9 Apr 2005 20:32:57 -0700

N. Silver wrote:

> *Rick Decker wrote:*

> > *JSH wrote:*

>

> > > *How would you know which way to go?*

>

> > *That's immaterial, as you imply. The problem still remains that*

> > *your theorem...*

>

> *Decker writes "your" as opposed to "the" so he doesn't have to*

> *put quotes around the word "theorem."*

>

Your reply is childish.

Nothing specific, just a slash at the idea it's a theorem without giving any support for your position.

> > *presented in your paper (which might be correct,*

> > *though there are two unimportant errors in your exposition and one*

> > *unproved assertion) still has no proof that the "rational factors"*

you

> > *find actually give any reliable nontrivial integer factors of M.*

>

> *which is the whole ball game.*

>

Not really, as in factoring, for years a difference of squares has been important, while the surrogate factoring theorem gives you an *infinite* number of solutions to a difference of squares with your target.

That is just given, as you take factors of T_j^2 , and as you can take rational factors, you have an infinite supply, and for *each* set of factors f_1 and f_2 such that

$$f_1 f_2 = T_j^2$$

you get factors g_1 and g_2 such that

$$g_1 g_2 = TM^2$$

where M is your target.

So the theorem as it is gives you what has never before been seen, guaranteed an infinite supply of potentially non-trivial solutions to a difference of squares.

> > *Fix that and you might have something.*

>

> *If you can prove something, you might have a proof.*

Words. I present a theorem, and posters go through a lot of social effort to hide it as that is the real math world.

It's about fluff and stuff.

Think about it. Mathematicians TELL people the factoring problem is hard because they can't figure it out. Mostly mathematicians or people trained by mathematicians or using tools used by mathematicians work to factor numbers.

The world takes on this system believing it secure.

But my collegework was training to be a physicist as my B.Sc. is in physics, so I was trained to challenge and not to follow lock-step.

I was trained for the discipline of physics.

Most people from the physics world don't bother with coming over to work on "pure math" problems, but I found myself focusing on them for many reasons.

The physics world trains you to solve problems.

It does not train you to accept that a problem is hard because people say so, or because no one else has found a simple solution.

I am a product of the physics world.

Math people are trained to believe that what can be simply done has already simply been done, so they are trained to look for complex solutions that build on ****what's already known**** and not to look for simple solutions, in "hard" areas, where they are told what is hard.

Math people are a herd.

So even easy problems are effectively hard because they convince themselves they are hard, and with most math people following along,

sci.crypt: Re: Gist of surrogate factoring theorem

you get a situation like what is facing the world today, where math people convinced themselves something was hard, and then convinced the world---or most of it.

They didn't convince me, so I went looking, and I found the surrogate factoring theorem.

James Harris