

# Re: What surrogate factoring theory now says

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00629.html>

---

- *From:* "Nomen Lapetos" <nospam@xxxxxxxxxx>
  - *Date:* Wed, 21 Mar 2007 00:25:54 -0500
- 

"Enrico" <ungererik@xxxxxxx> wrote in message  
<news:1174448963.111354.193940@xx>  
On Mar 20, 7:36?pm, jst...@xxxxxxxxxx wrote:

I want to emphasize that there can be a new factoring method that just takes a while to be fully engineered, as there is the theory and there is the engineering into a practical solution.

Like Isaac Newton knew difference of squares, but he didn't have the Number Field Sieve.

Surrogate factoring theory says that you can turn factoring a hard target  $T$ , into a problem of factoring an indefinite number of surrogates  $S_1, S_2, S_3, \dots$  making the problem potentially tractable.

My own target for my research is factoring an RSA sized number—of any bit length feasible—within ten minutes on a home computer.

That has been my research target for years now. The theory says that once the engineering is figured out that is achievable.

You can personally check the very simple underlying mathematics yourself.

(Web search on surrogate factoring, stay away from the old failed stuff though.)

Mainly I just added one more congruence to the difference of squares.

So it's not like the algebra is hard, or it's difficult to follow.

But just like with just the difference of squares, figuring out a practical solution could take a while, where I don't think it'll take centuries like with difference of squares to the NFS.

I am in the process of trying to turn what could take years of research from lots of people around the world into months or days of

## Re: What surrogate factoring theory now says

research where I am the primary engine, but I could fail, and others could succeed.

So, say, Russia could succeed. Or China could succeed. Or Iran could succeed. Or, maybe even North Korea could succeed.

Would my own country the United States?

Sure, but history says that people here might not bother because we're on the top of the heap.

People at the top tend to ignore "crackpot" ideas.

But I could be wrong, right? Lots of math people say I'm a crackpot and I've been babbling about surrogate factoring for YEARS, including in the past having said that I'd solved the factoring problem, when I hadn't.

Yup. I've failed a lot. I admit it. But I've succeeded a lot, and "mathematicians" won't admit it.

Roll the dice and the fate of the world could change.

That's how it's happened before...people like you under-rate the power of ideas despite thinking you're idea people, and you ignore something you DECIDE is dinky and worthless, and civilization itself changes.

If that didn't happen, no dominant country would ever lose that position. We might be under the Persian Empire, or the Roman or the Egyptian or some other if people just learned not to underestimate the power of ideas.

Then again, I could be wrong. I don't think I am, but I have been wrong before.

But hey, it's mathematics!!! I say, don't trust me. I don't trust you, or I wouldn't be making this post. I think most of you are complacent idiots who would let the world go up in flames because you're too small-minded and maybe corrupt to really care, and I don't trust you.

Go with the math.

If I'm right, it says I'm right. If I'm wrong, it says I'm wrong.

If it says I'm right, and you think you can just play the odds that no one in the world will figure this out, not Russia, not China, not anybody, and you're wrong...well, welcome then to a Brave New World, and yet another example that history repeats...

James Harris

## Re: What surrogate factoring theory now says

Hey, James!

You don't have to factor each surrogate from scratch.

If prime  $P$  divides  $2k^2 + wT$  then

prime  $P$  also divides  $2(k+PX)^2 + (w + PY)T$

where  $X, Y$  are any integers.

This shows up best on Excel with  $k$  varying on the horizontal and  $w$  varying on the vertical – each surrogate is calculated at the intersection and its value mod  $P$  is taken with conditional formatting used to highlight the 0 values.

Any  $P$  by  $P$  region will tessellate the whole plane, so its easy to set up a sieve to strain out the small primes.

Enrico

\*\*got an example you could attach, or post in text?

.