

Proper evaluation of surrogate factoring

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00102.html>

- *From:* jstevh@xxxxxxxxxx
 - *Date:* 2 Mar 2007 14:42:55 -0800
-

Surrogate factoring is just kind of a wild idea that means you have to think carefully to understand how to evaluate its effectiveness.

Mathematically it reduces to solving two congruence relations:

$$x^2 = y^2 \pmod{T}$$

and

$$k^2 = 2xk \pmod{T}$$

where the first should be familiar as it's just the well-known congruence of squares, while the second is what you need mathematically to add to get to what I call surrogate factoring.

To use surrogate factoring you pick k , and then everything you do is determined as you can only then move in increments of T , your target composite to get your surrogate which is factored.

Moving from congruences to explicit equations you find that surrogate is $2k^2 + wT$, with w a non-zero integer, where you can see that once k is picked you can only move in multiples of T .

Work the theory.

What never gets mentioned in discussions is the answer to the question, what mathematically should you expect using that system of equations?

It's not discussed as the theory all supports me.

So posters have to go to other means, like, how do you evaluate factoring efficiency with the classical methods?

Those are searches so you just go by how many attempts you make versus successes.

But with surrogate factoring, theory shows easily that for ANY k , there exists a family of solutions for x and y , your difference of

Proper evaluation of surrogate factoring

squares, and you can only change the surrogate that is factoring in multiples of T , so what does the theory indicate about the probability of factoring?

Oddly enough it indicates that you should have about a 25% to 50% probability of factoring with ANY non-zero k that you choose, with a k/T ratio of higher than 5%.

That's weird. It requires thinking about factoring success in a different way than before, where the focus is on k , not on all the combinations for a particular k that do not work.

Now if that 25% to 50% probability holds up, you have a method that could blow away everything else, though it does need help in that you have to factor that surrogate, which is why there can be a nasty pause where nothing seems to be happening in this area in terms of it being picked up around the world.

The pause can be because the surrogate can be somewhat hard to factor.

And the surrogate inevitably gets bigger as T increases in size, so you need a research team that can already do some serious factoring to get it useful for the really big numbers—if it can be made useful.

Theory says it can. The theory shows no impact from the size of T , except on the k/T ratio where the optimal ratio steadily rises as the size of T increases, where I give the optimal and the basic theory—it is easy—on my Extreme Mathematics group:

<http://groups.google.com/group/extrememathematics/web/surrogate-factoring>

A major problem I think for most of you when it comes to understanding the implications of surrogate factoring is that you depend on mathematicians, who lie a lot.

I am being very serious here, modern mathematicians lie a lot.

They lie for their own personal interests, and here they feel a need to preserve the current system which gives them prestige and jobs with people believing that systems based on factoring being a hard problem are safe.

They are cons, so why should they suddenly care about people here and now just because lots of money could be at stake and people could be destroyed by their lies?

I assure you they do not care now any more than before.

They will lie about surrogate factoring like everything else, so check the easy algebra.

Proper evaluation of surrogate factoring

Mathematical proof is the easy part, but countering faith in cons is very, very hard.

Many modern mathematicians lie all the time about mathematics.

It's how they stay in business.

James Harris

.