

Re: Magic Flight: A New Public Key Algorithm stronger? than factoring

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/0592.html>

From: Jim Steuert (pjsteuert_at_rcn.com)

Date: 07/09/03

Date: Tue, 08 Jul 2003 18:17:54 -0400

Bryan Olson wrote:

>

> *an inverse. It might be an interesting exercise to prove or*
> *disprove that for any (commutative) ring, there's always a*
> *linear combination of rows that provides a pivot.*

>

> *No problem: use the row beginning with '2' as the pivot.*

No it is a problem. It is the crux of the problem.

I'm not surprised that you found pivots for this tiny example.

But what if there is another "isolated" set of values
say, t , which like 4, map only into t or u .

Then "no" pivot will clear that entire column. Then you
do not have upper-triangular at all.

You have not demonstrated that Gaussian Elimination can
be used with commutative rings when some values are without
multiplicative inverses.

In fact, commutative rings needn't have any multiplicative
inverses. Values can just multiplicatively cycle (which may be an
advantage for this usage, as it may make Gaussian Elimination
a combinational explosion) in disjoint sets of values (ideals).
(but still come out of the cycles additively)

And again, that is the crux of the original problem, which you have
just deferred to another problem, without solving it.

I still suspect that it is a combinational problem. That is what motivated
this "lossy" idea.

-Jim

sci.crypt: Re: Magic Flight: A New Public Key Algorithm stronger? than factoring

On Tue, 08 Jul 2003 21:06:55 GMT, Bryan Olson <fakeaddress@nowhere.org>
wrote:

> *Jim Steuert wrote:*
>>
>> *Francois Grieru wrote:*
>>
>>> *Knowing M and $alices_public$, by Gaussian elimination or some
>>> faster method, it is easy to find one of the (possibly several)
>>> $alices_secret$ that match this equation.*
>>
>> *Gaussian elimination requires that values have
>> multiplicative inverses. The basic operation is row-reduction – some
>> constant times one row added to the other row makes zero.*
>>
>> $k*(4\ x\ x\ x\ x\ \dots)$
>> $+(2\ y\ y\ y\ y\ \dots)$
>> $\Rightarrow (0\ z\ z\ z\ z\ \dots)$
>>
>> *My problem is that $k*4$ is not "ever" equal to 2.
>> If values all had inverses this would be easy.
>> Just form $k = -(4^e - 1)*2$, and you're done.*
>
> *No problem: use the row beginning with '2' as the pivot. For
> mod 2^n arithmetic in general, use a term where the number of
> factors of 2 is minimal.*
>
>
>> *In the tabular commutative ring example
> [...]
>> If it could always be reordered so that
>> the values with inverses are done first, but then the problem
>> remains with the other rows... Re-ordering schemes could end
>> up in circular loops.*
>
> *Upper-triangular form is fine, and you never have to
> un-re-order.*
>
> *Note that re-ordering doesn't always work. For example, if we're
> working mod-15, we might get to a column:*
>
> 3, ...
> 5, ...
> 9, ...
> 10, ...
>
> *None of the terms divides all the others. Still not a problem:
> we simply add the second row into the first to get a pivot with
> an inverse. It might be an interesting exercise to prove or
> disprove that for any (commutative) ring, there's always a
> linear combination of rows that provides a pivot.*

sci.crypt: Re: Magic Flight: A New Public Key Algorithm stronger? than factoring

>

>

--

Using M2, Opera's revolutionary e-mail client: <http://www.opera.com/m2/>