

## Re: A new public key algorithm based on avalanche properties

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/0045.html>

---

**From:** Jim Steuert ([pjsteuert\\_at\\_rcn.com](mailto:pjsteuert_at_rcn.com))

**Date:** 07/01/03

Date: Tue, 01 Jul 2003 00:30:23 -0400

Tom St. Dennis said:

>

> *Actually there are no inverses if the determinant is not a unit.*

>

Hi Tom,

You are correct. The definition of unit is that it has an inverse. The determinant of such a value must be a unit, since the formula for inverse involves  $\text{determinant}^{-1}$ . It is not enough for it to be non-zero. The additive zero is just a special case. And I don't claim to be an abstract algebra expert, although I have picked up pieces here and there when I'm interested.

Still, I believe that the much simpler avalanche-based public key exchange algorithm (which I have coded and tested as well) in my post earlier today is secure, although it is not based on commutative algebra at all. It is entirely based on the mixers being homomorphic transformations and the idea of hiding the  $x_{\text{global}}$  in the middle of the avalanche.

What I was discussing about rings was my "other" public key algorithm ideas based on commutative rings. The mixers in the avalanche.c algorithm are not commutative (they don't need to be for avalanche only), and my original pdf diagram was wrong in that it was not really commutative. A "commutative" mixer would be a 2-input, 2-output mixer like:

$(x',y') = (a,b)*(x,y) = (ax+by, -bx+ay)$  in the  $a+b*\text{sqr}(-1)$  ring  
or like:

$(x',y') = (a,b)*(x,y) = (a+b*\text{sqr}(17))*(x+y*\text{sqr}(17)) = ( a*x+17*b*y, a*y+b*x )$

in the  $a+b\sqrt{17}$  ring.

where by "commutative" one can follow one multiplication operation say, by (a,b) with another by (c,d) and the result is the same as if you multiplied by (a,b) and then followed by (c,d). So that multiplication is commutative. No two-input one-output mixer can ever be commutative in that sense.

This "other" public key algorithm is based on the observation that a commutative ring for which some values are not units (have no inverse) can be used to create complex functions which are not easily invertible, either in a alice/bob commutative sense, or in an avalanche, by using this as the basic multiplication mixer operation, and then things like  $a+b\sqrt{17}$  as a ring where a and b are defined as the tabular "lossy" 3-bit commutative ring elements (see included tables below).

Likewise, an 8-input/8-output commutative ring mixer could be defined as multiplication of two or more 8-dimension vector quantities like:

$$v = a+b\sqrt{q}+c\sqrt{r}+d\sqrt{s}+e\sqrt{qr}+f\sqrt{qs}+g\sqrt{rs}+h\sqrt{qrs}$$

where multiplication by another 8-part vector is the mixing operation.

and where q, r, and s are primes, and where the 8 values a,b,c,d,e,f,g,h are themselves ring elements defined as above, or with another commutative ring definition like the 3-bit tabular one below. That is what I meant by "nested definition" of rings. This is just some interesting rings I found in Schaum's, as applied to this mixer idea. By virtue of this tabular ring not having multiplicative inverses, I "think" that would make this thing not easily divisible and thus the mixer would not be easily invertible (many-to-one).

I found the following tabular commutative ring in Schaum's outline series "Modern Abstract Algebra", for which b,e,f are not units, and  $e=g^{-1}$ ,  $d=d^{-1}$ ,  $g=c^{-1}$ , and  $h=h^{-1}$  are units (a is the zero), and h is the multiplicative unity. It can be used to encode 3-bit values.

```

+ abcdefgh
-----
a|abcdefgh
b|badcfegh
c|cdefghab
d|dcfeghba
e|efghabcd
f|feghbadc
g|ghabcdef
h|hgbadcf

```

\* abcdefgh

-----  
a|aaaaaaaa  
b|aefbaefb  
c|afdgebhc  
d|abghefcd  
e|aaeeaaee  
f|aebfaebf  
g|afhcebdg  
g|abcdefgh

-Jim

On Tue, 01 Jul 2003 01:45:35 GMT, Tom St Denis <tomstdenis@iahu.ca> wrote:

> *Jim Steuert wrote:*

>> *Some of the rings in the sequence of definitions*  
>> *are "lossy" in the sense that there is no multiplicative*  
>> *inverse for some values. One example is the ring  $a + b\sqrt{17}$*   
>> *module  $2^k$ . That ring is isomorphic to the set of  $2 \times 2$  matrices*  
>> *of the form  $(a, b, 17b, a)$ . There is no inverse when the*  
>> *determinant  $(a^2 - 17b^2)$  is zero mod  $2^k$ . There are other*  
>> *more simple tabular examples.*

>

> *Actually there are no inverses if the determinant is not a unit.*

>

> *Might want to revise your algebra a tad :-)*

>

> *Tom*

>

> *[Coming from the person [me] who routine gets low marks in Algebra you*

> *may want to rethink your approach to cryptography as well!]*

>

>