

Re: XOR and ADD subtil difference ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-11/1470.html>

From: Arnaud Carré (arnaud.carreNOSPAM_at_freesurf.fr)

Date: 11/30/04

Date: Tue, 30 Nov 2004 15:49:00 +0100

> > *Other: AES uses plenty of XOR like many block cyphers. (let's say on
> 32bits
> > integer in 32bits implementation). What do you think of the security of
a
> > "modified" AES using ADD instead of XOR ??
>
> You mean ADD modulo something? ADD modulo what? ADD modulo 2^{32} ?*

oh yes sorry I don't specify that. Of course I mean "modulo" add, and modulo the same size used by any XOR (with one bit register XOR is equivalent to ADD).

so in the AES 32bits implementation exemple, of course I speak about replacing integer 32bits XOR by integer 32bits ADD (so modulo 2^{32})

And don't be worried, that's not because I don't think XOR is not secure !! :-)
It's just therorical knowledge. I want to know if "modulo add" is as safe as XOR .

Any idea ?