

Re: OMAC help

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/0573.html>

From: Tom St Denis (tomstdenis_at_iahu.ca)

Date: 06/14/03

Date: Sat, 14 Jun 2003 16:58:14 GMT

Jack Lloyd wrote:

> *On Fri, 13 Jun 2003 18:29:05 -0400, Brian Gladman wrote:*

>

>

>> *Maybe I am missing something but they seemed almost the same in software*

>> *- just two small code sequences (gf_mulx & gfdivx) in place of one*

>> *(gf_mulx). Is there more to it than this?*

>

>

> *Nope. The part I like about it is you don't have to remember (or*

> *calculate) what the inverse of the polynomial is, only the poly*

> *itself. Perhaps I overstate OMAC1's advantages, but I've always*

> *had a hard time with polynomial arithmetic for some reason, so*

> *anything that reduces how much of it I have to think about is a*

> *good thing to me. (Also, anything that reduces code size at no cost ==*

> *good).*

Personally I don't see the benefit of OMAC at all. It is **not** a combined encrypt/mac algorithm [it requires you to decrypt and re-encrypt to verify the mac as far as I can tell].

The specs are horrible. Admittedly I don't have 30 yrs in the field but I have implemented some hairy algorithms [Twofish, CAST5, etc..] before and this one perplexes me. I spent a good 8 hours toying with it and everytime I failed to produce correct output.

Personally I just think the specs are half-assed. They spent too much time analyzing the algorithm and not enough describing how to implement it [hint: reference source code would have gone a long way!]

I don't see the advantage over say HMAC. In fact I was quite horribly surprised that a non-encrypt mode was picked....

Oh well back to CTR+HMAC for me :-)

Tom