

Re: Dr. Brian Gladman -- does anyone know how to contact him?

Re: Dr. Brian Gladman -- does anyone know how to contact him?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-02/msg00915.html>

- *From:* "usenet.plus.net" <brg@xxxxxxxxxxxxx>
 - *Date:* Wed, 27 Feb 2008 08:27:57 -0000
-

<johnsmith080226@xxxxxxxxxxxxx> wrote in message
news:2739fec2-3b2c-4612-bdad-48152bccb662@xx

Hello,

I know that Dr. Brian Gladman sometimes posts to sci.crypt. I need to email him (can't discuss the matter publicly), but I couldn't find his email address on his site. The readme files accompanying his source code don't contain any contact details either (which kind of surprised me because he wrote that he needs feedback).

Can anyone help me? I can be contacted at this disposable email address: johnsmith080226@xxxxxxxxxxxxx

I don't know how to solve the email address problem. A throw away address doesn't help much.

And when I had my email address in my code and on my web site, even when obfuscated, I still ended up with a huge amount of spam. So I now make it a bit more difficult to obtain but googling gets it quite easily (do an obvious google search plus 'gsl' for example).

My thanks to other responders for mentioning my request for help with some newly released code. The Galois field $GF(2^{128})$ is used in many crypto mode algorithms but, sadly, the field is represented differently in many of them. So I gave up and updated my $GF(2^{128})$ multiplier to be configurable for any of the four common field representations.

Although I have tested this on little endian systems, I don't have a big endian system so I would appreciate any help people might be able to offer in testing it on such systems.

I have a version of GCM that allows the field multiplier to be tested but I am afraid it's 'not a walk in the park' because there are 4 different field representations, 4 different table based optimisations and 3 different buffer optimisations – quite a few combinations. But it would help if even a few were tested on a big endian system (the buffer optimisations are the most likely to fail).

Brian Gladman

.

Re: Dr. Brian Gladman -- does anyone know how to contact him?