

Re: David's authenticated encryption mode.

Re: David's authenticated encryption mode.

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01678.html>

- *From:* Mark Wooding <mdw@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 31 Aug 2006 00:57:29 +0000 (UTC)
-

Mike Amling <nospam@xxxxxxxx> wrote:

We might note that the Helix stream cipher that Greg Rose cites has since been superseded by the Phelix stream cipher.

Indeed it has: thanks for pointing that out. Also, the paper predates GCM. It can be found at

<http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-revised-spec.pdf>

-- [mdw]

.