

Re: counter mode and data integrity

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3070.html>

From: Joerg Platte (Joerg.Platte_at_uni-dortmund.de)

Date: 10/31/03

Date: Fri, 31 Oct 2003 13:38:44 +0100

John E. Hadstate wrote:

- > *If I understand your proposal, you want to use part of a hash of the block*
- > *data concatenated with a block address as the counter in CTR mode. You*
- > *would then encipher the block data using the CTR-mode ciphertext.*
- >
- > *My question is, how do you decipher the data? You need the plaintext to*
- > *compute the hash that makes-up part of your counter. If you don't have*
- > *the plaintext available, with what do you feed the counter?*

The counter (hash value) can be stored with the corresponding block. There is no need to encrypt or protect the counter value. So it's possible to decipher the block with this counter and the secret AES key.

regards,
Jörg

--

Dipl.-Ing. Jörg Platte
Computer Engineering Institute | phone: +49 231-755-6165
University Dortmund | mobile: +49 178-2978865
44221 Dortmund / Germany | fax: +49 231-755-3251