Dear all:
There is a small error in the reference implementation of Lotus.
When the nonce is mixed with the key, only CRYPTO_ABYTES of the nonce are used. As a result, the cipher behaves as one with a 64 bit-nonce, instead of the specified 128.

Best regards
Miguel Montes
From: Ashwin Jha <letterstoashwin@gmail.com>
Sent: Sunday, April 28, 2019 2:45 PM
To: lightweight-crypto; Miguel Montes
Cc: lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; cuauhtemoc.mancillas83@gmail.com; Mridul Nandi; sasaki.yu@lab.ntt.co.jp; Ashwin Jha
Subject: Re: [lwc-forum] OFFICIAL COMMENT: LOTUS-AEAD and LOCUS-AEAD
Attachments: lotus-aead_and_locus-aead_v1.tar.gz

Dear Miguel,

Thanks for pointing out the bug in the reference implementation of LOTUS-AEAD.

Dear all,

Specifically, the bug was at line 96 of encrypt.c file of LOTUS-AEAD implementation.

Incorrect version: "xor_bytes(nonced_key, nonce, CRYPTO_ABYTES);

Correct version: "xor_bytes(nonced_key, nonce, CRYPTO_NPUBBYTES);

We have fixed the bug in the reference implementation (also attached here).

NOTE: The bug pertains to the reference implementation and does not require any change in the specification of LOTUS-AEAD.

Regards,
LOTUS-AEAD and LOCUS-AEAD Team

On Sun, Apr 28, 2019 at 1:43 AM Miguel Montes <miguel.montes@gmail.com> wrote:
>
> Dear all:
> There is a small error in the reference implementation of Lotus.
> When the nonce is mixed with the key, only CRYPTO_ABYTES of the nonce are used. As a result, the cipher behaves as one with a 64 bit-nonce, instead of the specified 128.
> Best regards
> Miguel Montes
>
> --
> To unsubscribe from this group, send email to
> lwc-forum+unsubscribe@list.nist.gov
> Visit this group at
> https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum
> ---
> You received this message because you are subscribed to the Google Groups "lwc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to lwc-forum+unsubscribe@list.nist.gov.