From: Miguel Montes <miguel.montes@gmail.com>
Sent: Saturday, April 27, 2019 4:12 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Limdolen

Dear all:
There is a problem with the reference implementation of Limdolen 256.

The Limdolen 256 specification states:
"The 256-bit input and key are split into two equal halves; Input = {u, v}, Key = {k1, k2} and each half is passed through a single round function of the 128-bit construct. At the end of each round, the output {u', v'} is processed by XORing u' into v' and replacing u' with v' such that the round function output is {v', u'⨁v'}"

The reference implementation reuses the first 128 bits of the key for the second half of the input, so the last 128 bits of the key are ignored and never used.
Best regards
Miguel Montes

From: Carl Mehner <c@cem.me>
Sent: Monday, April 29, 2019 12:08 AM
To: Miguel Montes
Cc: lightweight-crypto; lwc-forum@list.nist.gov
Subject: Re: [lwc-forum] OFFICIAL COMMENT: Limdolen

Thank you Miguel,
I have updated the Limdolen 256 reference code to correct this error and have also updated the test vector output file, both on Limdolen's code repo.
-cem

Carl Mehner

On Sat, Apr 27, 2019 at 3:12 PM Miguel Montes <miguel.montes@gmail.com> wrote:

> Dear all:
> There is a problem with the reference implementation of Limdolen 256.
>
> The Limdolen 256 specification states:
> "The 256-bit input and key are split into two equal halves; Input = {u, v}, Key = {k1, k2} and each half is passed through a single round function of the 128-bit construct. At the end of each round, the output {u', v'} is processed by XORing u' into v' and replacing u' with v' such that the round function output is {v', u'⊕v'}"
>
> The reference implementation reuses the first 128 bits of the key for the second half of the input, so the last 128 bits of the key are ignored and never used.
> 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.

From: Raghvendra Rohit <iraghvendrarohit@gmail.com>
Sent: Friday, May 17, 2019 2:58 PM
To: Carl Mehner
Cc: Miguel Montes; lightweight-crypto; lwc-forum@list.nist.gov; samuel.c.p.neves@gmail.com
Subject: Re: [lwc-forum] OFFICIAL COMMENT: Limdolen
Attachments: encrypt.c

Dear all,

Apart from the full round differential distinguisher (for the underlying block cipher) found by Samuel Neves, it seems there are structural
weaknesses in Limdolen AEAD which leads to simple forgery attacks. Below are the short details and attached is the code for verification.

****
Forgery 1
****
1) Query (N, AD, M) to the encryption oracle where AD = ad_0||ad_1||ad_0||ad_1, |AD| = 4*128 and |M|=128 bit. Observe the (C, T) value.
2) Let AD' = 4*j concatenation of AD for j>=2. For example j = 2, implies AD' = ad_0||ad_1||ad_0||ad_1||ad_0||ad_1||ad_0||ad_1. Query (N, AD', C, T) to
the decryption oracle. This query will pass the verification with probability 1.

****
Forgery 2
****
1) Query (N, AD, M) to the encryption oracle where AD = ad_0||ad_1||ad_0||ad_1, |AD| = 4*128 and |M|=128 bit. Observe the (C, T) value.
2) Compute the first key stream byte z = M[0] ^ C[0]. Let C'[0] = M[15] ^ z and AD' = AD||M[0]||M[1].....||M[14]. Note that C' not equal to C and
AD not equal to AD'.
3) Query (N, AD', C', T) to the decryption oracle. Again, this query will pass the verification with probability 1.

**** Note that we can change any number of bytes in the last block and not just the last byte.**
**** Both the forgeries work for 256 bit version as well.**

Thanks and regards,
Raghav

On Mon, Apr 29, 2019 at 12:08 AM Carl Mehner <c@cem.me> wrote:

> Thank you Miguel,
> I have updated the Limdolen 256 reference code to correct this error and have also updated the test vector output file, both on Limdolen's code repo.
> -cem
>
> Carl Mehner
>
> On Sat, Apr 27, 2019 at 3:12 PM Miguel Montes <miguel.montes@gmail.com> wrote:
>
> > Dear all: