From: NILanjan Datta <nil.wid.frnds@gmail.com>
Sent: Thursday, April 25, 2019 11:33 AM
To: lwc-forum
Cc: mridul.nandi@gmail.com; ashwin.jha1991@gmail.com; lightweight-crypto
Subject: OFFICIAL COMMENT: Forgery against SIV-Rijndael256-AEAD and SIV-TEM-PHOTON-AEAD

Dear all,

We have found forgery against SIV-Rijndael256-AEAD and SIV-TEM-PHOTON-AEAD exploiting improper associated data processing.

If the message length is less than 128 bits, two queries with same padded associated data (one with full block and the other with partial) generates same (ciphertext, tag) pair. Formally, the following forging attack can be mounted on SIV-Rijndael256-AEAD:

1. Step 1: Construct A (|A|=256) and A' (|A'| < 256) such that pad(A) = pad(A').
2. Query (N,A,M), with |M| < 128. Let the (ciphertext, tag) pair be (C,T).
3. Forge with (N,A',C,T).

For SIV-TEM-PHOTON-AEAD, take length of A to be 384 and A' to be less than 384 bit and follow the same attack. We have verified both these attacks using the corresponding reference implementations.

Use of different tweaks (based on full / partial) during the final associated data block processing is a solution to this attack.

Thanks and regards,
Nilanjan Datta, Ashwin Jha and Mridul Nandi,
Indian Statistical Institute, Kolkata

From: Tetsu Iwata <tetsu.iwata@gmail.com> on behalf of Tetsu Iwata <iwata@cse.nagoya-u.ac.jp>
Sent: Friday, April 26, 2019 12:53 AM
To: NILanjan Datta; lwc-forum
Cc: mridul.nandi@gmail.com; ashwin.jha1991@gmail.com; lightweight-crypto
Subject: OFFICIAL COMMENT: Forgery against SIV-Rijndael256-AEAD and SIV-TEM-PHOTON-AEAD

Dear all,

We thank Nilanjan Datta, Ashwin Jha and Mridul Nandi for spotting the issue of the domain separation. The analysis is correct, and we will update the domain separation so that it works correctly, and will send the revision to the forum.

Best regards,

SIV-Rijndael256 and SIV-TEM-PHOTON team

On 2019/04/26 0:32, NILanjan Datta wrote:
> Dear all,
>
> We have found forgery against SIV-Rijndael256-AEAD and
> SIV-TEM-PHOTON-AEAD exploiting improper associated data processing.
>
> If the message length is less than 128 bits, two queries with same
> padded associated data (one with full block and the other with
> partial) generates same (ciphertext, tag) pair. Formally, the
> following forging attack can be mounted on SIV-Rijndael256-AEAD:
>
> 1. Step 1: Construct A (|A|=256) and A' (|A'| < 256) such that pad(A)
> = pad(A').
> 2. Query (N,A,M), with |M| < 128. Let the (ciphertext, tag) pair be (C,T).
> 3. Forge with (N,A',C,T).
>
> For SIV-TEM-PHOTON-AEAD, take length of A to be 384 and A' to be less
> than 384 bit and follow the same attack. We have verified both these
> attacks using the corresponding reference implementations.
>
> Use of different tweaks (based on full / partial) during the final
> associated data block processing is a solution to this attack.
>
> Thanks and regards,
> Nilanjan Datta, Ashwin Jha and Mridul Nandi, Indian Statistical
> Institute, Kolkata
>
> --
> 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.

From: Tetsu Iwata <tetsu.iwata@gmail.com> on behalf of Tetsu Iwata <iwata@cse.nagoya-u.ac.jp>
Sent: Tuesday, May 07, 2019 11:34 AM
To: NILanjan Datta; lwc-forum
Cc: mridul.nandi@gmail.com; ashwin.jha1991@gmail.com; lightweight-crypto
Subject: [lwc-forum] OFFICIAL COMMENT: Forgery against SIV-Rijndael256-AEAD and SIV-TEM-PHOTON-AEAD
Attachments: sivrijndael256v1.zip; sivtemphotonv1.zip; 00_siv-tem-photon.pdf; 00_siv-rijndael256.pdf

Dear all,

We have revised the document and the reference code so that the domain separation works correctly.
Change log is in the last page of the document.
We once again thank Nilanjan Datta, Ashwin Jha and Mridul Nandi for spotting the issue.

Best regards,

SIV-Rijndael256 and SIV-TEM-PHOTON team

On 2019/04/26 13:52, Tetsu Iwata wrote:
> Dear all,
>
> We thank Nilanjan Datta, Ashwin Jha and Mridul Nandi for spotting the
> issue of the domain separation. The analysis is correct, and we will
> update the domain separation so that it works correctly, and will send
> the revision to the forum.
>
> Best regards,
>
> SIV-Rijndael256 and SIV-TEM-PHOTON team
>
>
> On 2019/04/26 0:32, NILanjan Datta wrote:
>> Dear all,
>>
>> We have found forgery against SIV-Rijndael256-AEAD and
>> SIV-TEM-PHOTON-AEAD exploiting improper associated data processing.
>>
>> If the message length is less than 128 bits, two queries with same
>> padded associated data (one with full block and the other with
>> partial) generates same (ciphertext, tag) pair. Formally, the
>> following forging attack can be mounted on SIV-Rijndael256-AEAD:
>>
>> 1. Step 1: Construct A (|A|=256) and A' (|A'| < 256) such that pad(A)
>> = pad(A').
>> 2. Query (N,A,M), with |M| < 128. Let the (ciphertext, tag) pair be
>> (C,T).
>> 3. Forge with (N,A',C,T).
>>
>> For SIV-TEM-PHOTON-AEAD, take length of A to be 384 and A' to be less
>> than 384 bit and follow the same attack. We have verified both these