
From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Friday, May 29, 2020 5:42 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: ROUND 2 OFFICIAL COMMENT: HYENA

Dear all LWC members,
I hope you and your family are well in those difficult times.

It seems the round 2 version of Hyena is identical to the round 1 version ,and does not include the updated specification posted on April 27, 2019.
The round 2 version without the update is vulnerable to forgery.
The updated version from April 27,2019 is not vulnerable.

Source of vulnerability:

For a complete block the update of the variable Δ is $\Delta \leftarrow 2^t \odot \Delta$, with $t = 2$ if the last block of M is complete, or 3 if fractional. If a full block message is shortened by one block and the last block is made incomplete, then the same Δ is reused for the last block of the full message and the last block of the shortened message. This leads to potential forgery.

Detailed attack:

Considering a first known ciphertext message :
 $\{C, T\} = E(k, N, A, M)$

with $M = M_0 || M_1 || M_2$ and $C = C_0 || C_1 || C_2$, with M_1 and M_2 full blocks, and M_0 any message of full blocks.

M_{1_l} is the left half of M_1
 M_{2_l} is the left half of M_2

M_{1_r} is the right half of M_1
 M_{2_r} is the right half of M_2

Let's define a message with

$M_{forge} = M_0 || (M_{1_l} \text{ xor } C_{1_l} \text{ xor } C_{2_l}) || \text{trunc}(M_{2_r})$
with $\text{trunc}(x)$ the truncation the block x with last byte removed.

Then we can forge $E(k, N, A, M_{forge})$ with

$\{C_0 || C_{2_l} || \text{trunc}(M_{2_r} \text{ xor } M_{1_r} \text{ xor } C_{1_r}), T\}$

Key = 08831A952CA73EC940DB52ED64FF7601

Nonce = F03674BAF83E7C4280C6044A

PT = 29543190FA7867BA0000000000000000

AD =

CT = 5D2833F76A3C739F FFCB95B5FE9A75 93C150F0BD5A544732396458D5CEB50F

From: lwc-forum@list.nist.gov on behalf of NILanjan Datta <nil.wid.frnds@gmail.com>
Sent: Saturday, May 30, 2020 5:09 AM
To: lwc-forum
Cc: lightweight-crypto
Subject: [lwc-forum] Re: ROUND 2 OFFICIAL COMMENT: HYENA
Attachments: main.pdf

Dear Alexandre,

Hope you are doing well. Thanks a lot for showing interest and analyzing our design.

We would like to clarify that we had already identified the mistake in Algorithm Proc_TXT [Line: 10] where the value 2^t should have been replaced by 3^t and informed it in the lwc-forum group mail dated April 29, 2019 (depending on the time zone) with the proposed modification. However, the updated version was not considered in the 2nd round submission due to the competition policy of NIST. Given that the submission proceeds to the next round, we will consider the same update. The attack that you have presented is on the initial version and has exploited the overlooked mistake.

We would also like to mention that we have analyzed the updated version and this version of HyENA (spec + security analysis + FPGA H/W implementation results) has recently been accepted in the ToSC Special Issue on Designs for the NIST Lightweight Standardisation Process. You can find the paper attached with the mail.

Please let us know, if you need any information from us.

Thanks and regards,
Designers, HyENA

On Saturday, 30 May 2020 03:12:40 UTC+5:30, alexandre.mege wrote:

Dear all LWC members,

I hope you and your family are well in those difficult times.

It seems the round 2 version of Hyena is identical to the round 1 version ,and does not include the updated specification posted on April 27, 2019.

The round 2 version without the update is vulnerable to forgery.

The updated version from April 27,2019 is not vulnerable.