From: Ashwin Jha <letterstoashwin@gmail.com>
Sent: Friday, April 26, 2019 8:34 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; Ashwin Jha; Mridul Nandi
Subject: OFFICIAL COMMENT: HYENA
Attachments: hyena_v1.tar.gz; hyena_v1_changelog.pdf

Dear all,

We have found a minor typographical error in the specification of HyENA. In line 10 of "Proc_TXT" we used "2^t" (incorrect) instead of "3^t" (correct).

We have made this small correction in the revised specification. This change is also reflected in the reference implementation as well as the test vectors.

Please find attached the change log specifying the typo and the correction, and the updated reference implementation.

--
Regards,
HyENA Team

Change Log to HyENA

Avik Chakraborti, Nilanjan Datta, Ashwin Jha and Mridul Nandi

April 26, 2019

We have found a minor typo in the specification as given in Figure 2.4, where we had written 2 instead of 3. The exact modification is given below:

Algorithm Proc_TXT($X, \Delta, D, \mathsf{dir}$), Line 10:
"$\Delta \leftarrow 3^t \odot \Delta$" (correct version) instead of "$\Delta \leftarrow 2^t \odot \Delta$" (incorrect version).

Corresponding modification is also reflected in the reference implementation and test vectors.

From: Thomas Peyrin (Assoc Prof) <thomas.peyrin@ntu.edu.sg>
Sent: Friday, April 26, 2019 10:52 AM
To: Ashwin Jha; lightweight-crypto
Cc: lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; Ashwin Jha; Mridul Nandi
Subject: RE: [lwc-forum] OFFICIAL COMMENT: HYENA

Hi Ashwin,

Your typo is not only present in your reference implementation and in your algorithm description of Figure 2.4, but also in the figure description 2.1, no ?

Cheers,

Thomas.

-----Original Message-----
From: Ashwin Jha [mailto:letterstoashwin@gmail.com]
Sent: Friday, 26 April, 2019 20:34
To: lightweight-crypto@nist.gov
Cc: lwc-forum@list.nist.gov; avik chakraborti <avikchkrbrti@gmail.com>; Nilanjan Datta <nilanjan_isi_jrf@yahoo.com>; Ashwin Jha <ashwin.jha1991@gmail.com>; Mridul Nandi <mridul.nandi@gmail.com>
Subject: [lwc-forum] OFFICIAL COMMENT: HYENA

Dear all,

We have found a minor typographical error in the specification of HyENA. In line 10 of "Proc_TXT" we used "2^t" (incorrect) instead of "3^t" (correct).

We have made this small correction in the revised specification. This change is also reflected in the reference implementation as well as the test vectors.

Please find attached the change log specifying the typo and the correction, and the updated reference implementation.

--
Regards,
HyENA Team

--
To unsubscribe from this group, send email to lwc-forum+unsubscribe@list.nist.gov

From: Mridul Nandi <mridul.nandi@gmail.com>
Sent: Friday, April 26, 2019 11:00 AM
To: Thomas Peyrin (Assoc Prof)
Cc: Ashwin Jha; lightweight-crypto; lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; Ashwin Jha
Subject: Re: [lwc-forum] OFFICIAL COMMENT: HYENA

Dear Thomas,

Thanks for pointing out the issue in the figure .. yes, you are right.. This has to be reflected in the figure, too.. We will circulate the revised document in the forum..

Thanks and regards,
Mridul Nandi
Associate Professor
Indian Statistical Institute
Kolkata

On Fri, Apr 26, 2019 at 8:22 PM Thomas Peyrin (Assoc Prof) <thomas.peyrin@ntu.edu.sg> wrote:
>
> Hi Ashwin,
>
> Your typo is not only present in your reference implementation and in your algorithm description of Figure 2.4, but also in the figure description 2.1, no ?
>
> Cheers,
>
> Thomas.
>
>
> -----Original Message-----
> From: Ashwin Jha [mailto:letterstoashwin@gmail.com]
> Sent: Friday, 26 April, 2019 20:34
> To: lightweight-crypto@nist.gov
> Cc: lwc-forum@list.nist.gov; avik chakraborti
> <avikchkrbrti@gmail.com>; Nilanjan Datta <nilanjan_isi_jrf@yahoo.com>;
> Ashwin Jha <ashwin.jha1991@gmail.com>; Mridul Nandi
> <mridul.nandi@gmail.com>
> Subject: [lwc-forum] OFFICIAL COMMENT: HYENA
>
> Dear all,
>
> We have found a minor typographical error in the specification of HyENA. In line 10 of "Proc_TXT" we used "2^t" (incorrect) instead of "3^t" (correct).
>
> We have made this small correction in the revised specification. This change is also reflected in the reference implementation as well as the test vectors.
>
> Please find attached the change log specifying the typo and the correction, and the updated reference implementation.

From: Ashwin Jha <letterstoashwin@gmail.com>
Sent: Sunday, April 28, 2019 2:05 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; Mridul Nandi
Subject: OFFICIAL COMMENT: HYENA
Attachments: hyena_v1_spec.pdf; hyena_v1.tar.gz; hyena_v1_changelog.pdf

Dear all,

We have a minor modification in the specification of HyENA as given in Figure 2.4, where in Algorithm Proc_TXT [Line: 10], the value 2^t is replaced by 3^t. Corresponding modification is also reflected in Figure 2.1 and the reference code. Please refer to the attached files for details. The change log can also be found on page 11 of the specification file.

Regards,
HyENA Team

Change Log to HyENA

Avik Chakraborti, Nilanjan Datta, Ashwin Jha and Mridul Nandi

April 28, 2019

The updated draft contains the following modification in the specification as given in Figure 2.4, where we had written 2 instead of 3. The exact modifications are given below:

1. Algorithm Proc_TXT$(X, \Delta, D, \mathsf{dir})$, Line 10:

   "$\Delta \leftarrow 3^t \odot \Delta$" (correct version) instead of "$\Delta \leftarrow 2^t \odot \Delta$" (previous version).

2. The above modification requires the following change in the masking value corresponding to the final HYFB+ block in Figure 2.1:

   "$3^2 2^{a+m}$" (correct version) instead of "2^{a+m+2}" (previous version).

3. Corresponding modification is also reflected the reference implementation and the test vectors.