From: nasoor bagheri <na.bagheri@gmail.com>

Sent: Monday, May 06, 2019 3:20 AM

To: lwc-forum@list.nist.gov

Cc: Danilo Gligoroski; sadegh sadeghi; Majid Mahmoudzadeh Niknam

Subject: [lwc-forum] Official comment:GAGE AEAD

Dear All,

In GAGE, in the aead mode, we have |T|=128. On the other hand, for some variants, i.e. b=234 and b=240, b- |T| In such case, given T, the adversary can just guess the remaining part to recover the state and so do a forgery attack, for example. Hence, we believe the claimed security in table 2.1, for these variants are not correct.

Best Regards,

Nasour Bagheri, Sadegh Sadeghi and Majid Niknam

--

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

From: Danilo Gligoroski <danilog@ntnu.no> Monday, May 06, 2019 5:58 PM Sent: To: nasoor bagheri; lwc-forum@list.nist.gov Cc: sadegh sadeghi; Majid Mahmoudzadeh Niknam Subject: [lwc-forum] Re: Official comment:GAGE AEAD Dear Nasour, Sadegh and Majid, Thank you for your continuous interest and analysis of GAGE and InGAGE. If I understand correctly your remark, your forgery attack by guessing the remaining part of the state assumes a "Nonce reuse", right? Regards, Danilo! On 06/05/2019 03:19, nasoor bagheri wrote: Dear All, In GAGE, in the aead mode, we have |T|=128. On the other hand, for some variants, i.e. b=234 and b=240, b- |T|< |T|. In such case, given T, the adversary can just guess the remaining part to recover the state and so do a forgery attack, for example. Hence, we believe the claimed security in table 2.1, for these variants are not correct.

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

Nasour Bagheri, Sadegh Sadeghi and Majid Niknam

Best Regards,

From: Sent: To: Cc: Subject:	nasoor bagheri <na.bagheri@gmail.com> Tuesday, May 07, 2019 2:46 AM Danilo Gligoroski lwc-forum@list.nist.gov; sadegh sadeghi; Majid Mahmoudzadeh Niknam [lwc-forum] Re: Official comment:GAGE AEAD</na.bagheri@gmail.com>
Dear Danilo,	
scenario: 1) given (A, T, N), a 2) then the adversa use the associated 3) Given the state, the complexity wo Please note that th respecting assump To us, to fix this po	reply. The presented remark works even in nonce respecting setting. e.g. consider the below ssuming P =0, i.e. empty plaintext, and A > b- T . ary guesses the missing b- T bits of the last permutation to retrieve the state, where it is possible to data A to filter wrong guesses. then it is easy to generate the valid (A, P, C, T, N) for any desired P. uld be 2^{b- T } which is less than 2^{ T } when T =128 and b=232 or b= 240. The user has not repeated the nonce and henceforth the above scenario does not violate the nonce tion. Doint, either the key should have been used in the last block, similar to some other schemes, or the all be reduced for those variants.
Please correct us if	are missing any point.
Best Regards, Nasour, Sadegh an	
On Tue, May 7, 20:	19 at 2:27 AM Danilo Gligoroski < <u>danilog@ntnu.no</u> > wrote:
Dear Nasour, Sado	egh and Majid,
Thank you for you	or continuous interest and analysis of GAGE and InGAGE.
If I understand co reuse", right?	rrectly your remark, your forgery attack by guessing the remaining part of the state assumes a "Nonce
Regards,	
Danilo!	
On 06/05/2019 03	3:19, nasoor bagheri wrote:
Dear All,	,

In GAGE, in the aead mode, we have |T|=128. On the other hand, for some variants, i.e. b=234 and

From:	Danilo Gligoroski <danilog@ntnu.no></danilog@ntnu.no>
Sent:	Tuesday, May 07, 2019 9:39 AM
То:	lwc-forum@list.nist.gov
Subject	Re: [lwc-forum] Re: Official comment:GAGE AEAD
Dear Na	sour, Sadegh and Majid,
Voc. wo	will undate the Table 2.1 for h=222 and h=240
res, we	will update the Table 2.1 for b=232 and b=240.
Thank y	ou very much for your valuable input,
Danilo!	
On 07/0	05/2019 02:46, nasoor bagheri wrote:
	Dear Danilo,
	Thank you for your reply. The presented remark works even in nonce respecting setting. e.g. consider the below scenario:
	1) given (A, T, N), assuming P =0, i.e. empty plaintext, and A > b- T .
	2) then the adversary guesses the missing b- T bits of the last permutation to retrieve the state, where it is possible to use the associated data A to filter wrong guesses.
	3) Given the state, then it is easy to generate the valid (A, P, C, T, N) for any desired P.
	the complexity would be $2^{b- T }$ which is less than $2^{ T }$ when $ T =128$ and $b=232$ or $b=240$.
	Please note that the user has not repeated the nonce and henceforth the above scenario does not
	violate the nonce respecting assumption. To us, to fix this point, either the key should have been used in the last block, similar to some other
	schemes, or the security claim should be reduced for those variants.
	Please correct us if are missing any point.
	Best Regards,
	Nasour, Sadegh and Majid
	On Tue, May 7, 2019 at 2:27 AM Danilo Gligoroski < danilog@ntnu.no > wrote:
	Dear Nasour, Sadegh and Majid,

Thank you for your continuous interest and analysis of GAGE and InGAGE.

From: nasoor bagheri <na.bagheri@gmail.com>

Sent: Tuesday, May 07, 2019 10:30 AM

To: Danilo Gligoroski

Cc: lwc-forum@list.nist.gov; sadegh sadeghi; Majid Mahmoudzadeh Niknam

Subject: Re: [lwc-forum] Re: Official comment:GAGE AEAD

Dear Danilo,

Thank you for the feedback.

Best Regards, Nasour, sadegh and Majid

On Tue, May 7, 2019, 6:09 PM Danilo Gligoroski < danilog@ntnu.no> wrote:

Dear Nasour, Sadegh and Majid,

Yes, we will update the Table 2.1 for b=232 and b=240.

Thank you very much for your valuable input,

Danilo!

On 07/05/2019 02:46, nasoor bagheri wrote:

Dear Danilo,

Thank you for your reply. The presented remark works even in nonce respecting setting. e.g. consider the below scenario:

- 1) given (A, T, N), assuming |P|=0, i.e. empty plaintext, and |A| > b-|T|.
- 2) then the adversary guesses the missing b- |T| bits of the last permutation to retrieve the state, where it is possible to use the associated data A to filter wrong guesses.
- 3) Given the state, then it is easy to generate the valid (A, P, C, T, N) for any desired P. the complexity would be $2^{b-|T|}$ which is less than $2^{|T|}$ when |T|=128 and b=232 or b=240. Please note that the user has not repeated the nonce and henceforth the above scenario does not violate the nonce respecting assumption.

To us, to fix this point, either the key should have been used in the last block, similar to some other schemes, or the security claim should be reduced for those variants.

Please correct us if are missing any point.

Best Regards, Nasour, Sadegh and Majid From: Danilo Gligoroski <danilog@ntnu.no>
Sent: Tuesday, May 07, 2019 7:48 PM

To: lightweight-crypto
Cc: lwc-forum@list.nist.gov

Subject: OFFICIAL COMMENT: GAGE and InGAGE

Dear all,

We have updated Table 1.4 and Table 2.1 in the document for GAGE and InGAGE and made some redacting changes.

The updated document can be taken from the newly register web page http://gageingage.org/ i. e. from http://gageingage.org/upload/GAGEandInGAGEv1.01.pdf

Algorithm specifications have not been changed.

Change log is also included in the document.

We thank Nasour Bagheri, Sadegh Sadeghi and Majid Niknam for their valuable input.

Best regards,

GAGE and InGAGE team

P.S. NIST people can now add a link for our website: http://gageingage.org/