From: hi@arnepadmos.com
Sent: Sunday, October 9, 2022 5:13 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: FINALIST OFFICIAL COMMENT: ASCON

Dear NIST,

Let me start by saying that I think Ascon would make a great selection for the NIST LWC standard. I do have several comments:

Ascon parameters -- While the 30 September 2022 status update about Ascon states that the authors 'consider both Ascon-128 and Ascon-128a to be equally well-suited and secure choices', during both the CAESAR and LWC competition, Ascon-128 has always been the primary recommendation in every version of the submitted specifications. I believe that Ascon-128 should remain the primary recommendation, as I think that 'late' changes of key decisions -- such as those made to Romulus -- are undesirable.

Sessions and ratcheting -- In the latest Xoodyak update, the authors emphasise 'that API flexibility is an important asset for a lightweight cryptographic primitive'. Specifically, they note the utility of support for sessions and rolling subkeys. In personal communication, the Ascon team has shared that intermediate tags and ratcheting can be implemented by reusing the MAC as the nonce and by using the non-masked half of the state as the new key. If Ascon is selected, I believe it would be useful to standardise such features in an additional publication (see below).

Feature parity with SHAKE -- One year after SHA-3 was standardised as FIPS 202, an extension defining modes of operation constructed around SHAKE was published as NIST SP 800-185. Key features of these modes are the support for tuples and customisation strings. In addition to support for sessions and ratcheting, Ascon can also benefit from such features.
As illustrated by BLINKER, Strobe, SHOE, and Cyclist, sponges can be the basis for simple, lightweight two-party half-duplex record protocols.
Support for tuples and customisation strings -- e.g. through additional domain separation constants and/or padding rules -- can disambiguate directionality, metadata, headers, and protocol types. Note that Ascon's mode, including these extensions, may also be useful for SHAKE.

Regards,
Arne

From: lwc-forum@list.nist.gov on behalf of Maria Eichlseder <maria.eichlseder@iaik.tugraz.at>
Sent: Monday, October 10, 2022 8:08 AM
To: lwc-forum@list.nist.gov
Cc: hi@arnepadmos.com
Subject: Re: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear Arne,

Thanks for your comments on Ascon and its use-cases.
We just want to clarify that Ascon-128 and Ascon-128a have not been changed since 2016, well before their selection in the CAESAR portfolio.
Both algorithms received their fair share of third-party analysis.
Therefore, we express in the update that we consider both equally suited for their target applications. CAESAR and NIST required the identification of a primary member of the family of AEAD schemes. For both competitions, we selected Ascon-128 as primary member, which it still is.

Best regards,
Maria (on behalf of the Ascon team)

From: Thomas Peyrin (Prof) <thomas.peyrin@ntu.edu.sg>
Sent: Tuesday, October 11, 2022 2:02 AM
To: hi@arnepadmos.com; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: RE: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear all,

as Romulus is mentioned in this message, we would like to react to the claim that "'late' changes of key decisions -- such as those made to Romulus -- are undesirable.", as we believe this is a clear mischaracterization of the situation.

First, we would like to recall that since the start of the competition Romulus candidate only had two changes:
1) the number of rounds of the internal primitive has been reduced due to a very large security margin, clearly established by numerous third-party cryptanalysis
2) some side-variants have been removed to simplify our proposal, and two provably secure modes have been added (a hash function Romulus-H and a leakage-resilient mode Romulus-T, both from already existing modes) and these additions have been officially announced more than 18 months ago (they conform with the NIST's deadlines, they are not late changes).

Besides, we believe adding new features is not an undesirable key change, it is up to the NIST whether these extra features are needed or not. In fact, we find really contradictory that the email author sees Romulus additions from 18 months ago as undesirable, while just after proposing to add new features for Ascon.

Finally, we emphasize that our main version mode has been the same since the start of the competition. In addition, we note that many finalists increased the number of rounds, changed significant parts or details of their mode, added/removed variants (Ascon is actually also one of them), etc. Thus, we find that the aforementioned sentence does not represent well reality.

Regards,

Thomas (on behalf of the Romulus team)

-----Message d'origine-----
De : lwc-forum@list.nist.gov <lwc-forum@list.nist.gov> De la part de hi@arnepadmos.com Envoyé : Monday, 10 October 2022 5:13 AM À : lightweight-crypto@nist.gov Cc : lwc-forum@list.nist.gov Objet : [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear NIST,

Let me start by saying that I think Ascon would make a great selection for the NIST LWC standard. I do have several comments:

Ascon parameters -- While the 30 September 2022 status update about Ascon states that the authors 'consider both Ascon-128 and Ascon-128a to be equally well-suited and secure choices', during both the CAESAR and LWC competition, Ascon-128 has always been the primary recommendation in every version of the submitted specifications. I believe that Ascon-128 should remain the primary recommendation, as I think that 'late' changes of key decisions -- such as those made to Romulus -- are undesirable.

From: hi@arnepadmos.com
Sent: Thursday, October 20, 2022 4:59 PM
To: Thomas Peyrin (Prof)
Cc: lightweight-crypto; lwc-forum@list.nist.gov
Subject: Re: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear Thomas,

I don't see how it is 'really contradictory' to advocate for stability of the primary members during a competition, while also noting that there is a future beyond competitions (otherwise we'd be stuck with AES and ECB, CBC, CFB, OFB, and CTR as specified in SP 800-38A). For this, flexibility is valuable -- as you also note in Romulus's specification.
Of course, Ascon's permutation wasn't designed to be hermetic, so it's an interesting question how confidence would be gained in such extra functionality. Conversely, as noted in the Jammin' on the deck paper, how deck functions could be implemented using a tweakable block cipher is also an open question, including how efficient these would be.

Nowhere in my message did I state any of the additions to Romulus to be undesirable. My comment on the changes to Romulus didn't refer to adding new features, but to the reduction in the number of rounds. I think this isn't 'a clear mischaracterization of the situation': as you also note, 'the number of rounds of the internal primitive has been reduced due to a very large security margin'. People can view this 40% reduction in the number of rounds and the concomitant 40% increase in performance as a wise choice (e.g., see the Too much crypto paper), but they could also perceive this, in light of the Dual EC saga, as NIST picking a weakened version of an ISO standard -- even if this is without basis. Just look at the discussions around the proposed changes to Keccak's capacity.

Regards,
Arne

On 2022-10-11 08:02, Thomas Peyrin (Prof) wrote:
> Dear all,
>
> as Romulus is mentioned in this message, we would like to react to the
> claim that "'late' changes of key decisions -- such as those made to
> Romulus -- are undesirable.", as we believe this is a clear
> mischaracterization of the situation.
>
> First, we would like to recall that since the start of the competition
> Romulus candidate only had two changes:
> 1) the number of rounds of the internal primitive has been reduced due
> to a very large security margin, clearly established by numerous
> third-party cryptanalysis
> 2) some side-variants have been removed to simplify our proposal, and
> two provably secure modes have been added (a hash function Romulus-H
> and a leakage-resilient mode Romulus-T, both from already existing
> modes) and these additions have been officially announced more than 18
> months ago (they conform with the NIST’s deadlines, they are not late
> changes).
>
> Besides, we believe adding new features is not an undesirable key
> change, it is up to the NIST whether these extra features are needed

From: hi@arnepadmos.com
Sent: Thursday, October 20, 2022 5:00 PM
To: Maria Eichlseder
Cc: lightweight-crypto; lwc-forum@list.nist.gov
Subject: Re: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear Maria,

Thank you for the clarification of your comments from the status update around the suitability of Ascon-128 and Ascon-128a for their target applications and use cases, as well as your clarification of the status of Ascon-128 as the primary member of the submission.

Regards,
Arne

On 2022-10-10 14:07, Maria Eichlseder wrote:
> Dear Arne,
>
> Thanks for your comments on Ascon and its use-cases.
> We just want to clarify that Ascon-128 and Ascon-128a have not been
> changed since 2016, well before their selection in the CAESAR
> portfolio. Both algorithms received their fair share of third-party
> analysis. Therefore, we express in the update that we consider both
> equally suited for their target applications. CAESAR and NIST required
> the identification of a primary member of the family of AEAD schemes.
> For both competitions, we selected Ascon-128 as primary member, which
> it still is.
>
> Best regards,
> Maria (on behalf of the Ascon team)
>

From: 'Thomas Peyrin (Prof)' via lwc-forum <lwc-forum@list.nist.gov>
Sent: Thursday, October 27, 2022 10:18 AM
To: hi@arnepadmos.com
Cc: lightweight-crypto; lwc-forum@list.nist.gov
Subject: RE: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear Arne,

This comparison seems misleading and deserves clarification.

"... but they could also perceive this, in light of the Dual EC saga, as NIST picking a weakened version of an ISO standard -- even if this is without basis. Just look at the discussions around the proposed changes to Keccak's capacity."

We stress that the updated Skinny-128/384+ is NOT a weakened version of Skinny-128/384: for Skinny-128/384+ we are only targeting 128-bit security, in contrary to Skinny-128/384 which is supposed to go up to 384-bit key potentially. All the rationale for this stems from publicly accessible third-party analyses, and has been already described and documented, please check the update document (available at https://sites.google.com/site/skinnycipher/security as well).
Skinny was created to provide an open, transparent, well-analyzed, academy-based alternative to Simon and Speck. Thus, insinuating that people would shout "backdoor !" and comparing this to Dual EC saga is ... groundless.

We should not give any credit to that and let this influence NIST decisions.

To not pollute this forum, this will hopefully be our last reply to that thread. Sorry for the digression from your original discussion.

Regards,

Thomas on behalf of the Romulus team.

-----Message d'origine-----
De : hi@arnepadmos.com <hi@arnepadmos.com> Envoyé : Friday, 21 October 2022 4:59 AM À : Thomas Peyrin (Prof) <thomas.peyrin@ntu.edu.sg> Cc : lightweight-crypto@nist.gov; lwc-forum@list.nist.gov Objet : Re: [lwc-forum] FINALIST OFFICIAL COMMENT: ASCON

Dear Thomas,

I don't see how it is 'really contradictory' to advocate for stability of the primary members during a competition, while also noting that there is a future beyond competitions (otherwise we'd be stuck with AES and ECB, CBC, CFB, OFB, and CTR as specified in SP 800-38A). For this, flexibility is valuable -- as you also note in Romulus's specification.