From:	Calik, Cagdas (IntlAssoc)
To:	Sonmez Turan, Meltem (Fed); McKay, Kerry A. (Fed); Chang, Donghoon (IntlAssoc); (b) (6) (b) (6) ; Bassham, Lawrence E. (Fed)
Subject:	RE: Overview of the Round 1 Candidates
Date:	Wednesday, August 7, 2019 11:55:51 AM

Below is the list of submissions I've identified that claim RUP security:

ASCON, ESTATE, LAEM, LOTUS-LOCUS, Oribatida, SIV-Rijndael256, SIV-TEM-Photon, Xoodyak

This has to be double-checked though, it was obtained by searching the specifications for the keywords "RUP, release, unverified".

Cagdas

From: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Sent: Tuesday, August 6, 2019 11:43 AM
To: Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Chang, Donghoon (IntlAssoc) <donghoon.chang@nist.gov>; Donghoon Chang (b) (6) Bassham, Lawrence E. (Fed) <lawrence.bassham@nist.gov>
Subject: RE: Overview of the Round 1 Candidates

Thanks for the link Cagdas.

I think Sbox classification is too specific to be added to this generic section, but this classification will be useful for the next round selection. I don't think we will eliminate any algorithm based on their side channel resistance in this round.

RUP security might be more suitable for this section. Are you volunteering to provide a paragraph on that? :)

Thanks,
Meltem

From: Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>
Sent: Tuesday, August 6, 2019 11:36 AM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Chang, Donghoon (IntlAssoc) <donghoon.chang@nist.gov>; Donghoon Chang (b) (6) Bassham, Lawrence E. (Fed) <lawrence.bassham@nist.gov>
Subject: RE: Overview of the Round 1 Candidates

Link to the document Meltem is referring to:
https://nistgov.sharepoint.com/:w:/s/LightweightCrypto/Edyy8hXEqtlFlFlkjcUFBqEBr-

FNWiq4AwlqY9DufrcDiQ?e=8Wvubk

I am (was) going to make a classification based on the S-boxes and whether they need lookups or they can be implemented with bitslice and/or constant-time implementations.

Another feature that can be added to the list below is Release of Unverified Plaintext security.

Cagdas

From: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Sent: Tuesday, August 6, 2019 11:19 AM
To: McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Chang, Donghoon (IntlAssoc) <donghoon.chang@nist.gov>; Donghoon Chang (b) (6) Bassham, Lawrence E. (Fed) <lawrence.bassham@nist.gov>
Subject: Overview of the Round 1 Candidates

Hi everyone,

I am working on the overview of the first round candidates section of the report. We want to give a two-page summary/highlights about the candidates. I appreciate if you can contribute.

- Can at least one of you verify that my classification in Table 2 is correct?
- Can one of you provide the list the AES based (or AES inspired) submissions?
- Anything we want to say for tweakable BC vs BC – based designs?
- Anything we want to say about modes of operations?
- Anything we want to say about different design approaches, design rationale etc. ?
- Nonce-misuse resistance, quantum resistance

We may also want to reply to the Hardware API related discussion at the forum. Larry is on travel this week.

Thanks,
Meltem