From:	Sonmez Turan, Meltem (Assoc)
To:	Calik, Cagdas (IntlAssoc); lightweight-crypto
Subject:	RE: Draft - Announcing the NIST LWC second-round candidates
Date:	Friday, August 30, 2019 1:25:28 PM

Thanks Cagdas, I am fine with all suggestions. Kerry?

From: Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>
Sent: Friday, August 30, 2019 1:24 PM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; lightweight-crypto <lightweight-crypto@nist.gov>
Subject: RE: Draft - Announcing the NIST LWC second-round candidates

Here are my suggestions:

- all candidate submission teams -> all submitters
- the strongest submissions -> more promising candidates
- the decision process and rationale for the selection -> selection process / rationale for the selection
- No major design changes will be accepted -> No design changes will be accepted
- We estimate that the second round will last 12 months -> The second round is expected to last 12 months (this sentence belongs more to the previous paragraph)
- is planning to host -> will be hosting

Cagdas

From: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Sent: Friday, August 30, 2019 9:58 AM
To: lightweight-crypto <lightweight-crypto@nist.gov>
Subject: Draft - Announcing the NIST LWC second-round candidates

Any comments? We can send it around 3PM.

/****/

Dear subscribers of the NIST Lightweight Cryptography forum,

We would like to thank all candidate submission teams for their efforts in this standardization process. We would also like to thank those in the cryptographic community who have analyzed the proposals and shared their comments officially, through the forum, or published papers on various technical aspects of the candidates.

Due to the large number of submissions and the short timeline of the NIST lightweight cryptography

standardization process, NIST has decided to eliminate some of the candidates from consideration early in the first evaluation phase in order to focus analysis on the strongest submissions.

The second-round candidates of the NIST LWC standardization process are:

ACE	ASCON	COMET	DryGASCON
Elephant	ESTATE	ForkAE	GIFT-COFB
Gimli	Grain-128AEAD	HYENA	ISAP
KNOT	LOTUS-AEAD & LOCUS-AEAD	mixFeed	ORANGE
Oribatida	PHOTON-Beetle	Pyjamask	Romulus
SAEAES	Saturnin	SKINNY-AEAD/-HASH	SPARKLE (SCHWAEMM and ESCH)
SPIX	SpoC	Spook	Subterranean 2.0
SUNDAE-GIFT	TinyJambu	WAGE	Xoodyak

NIST will soon publish a report on the decision process and rationale for the selection at https://csrc.nist.gov/Projects/Lightweight-Cryptography .

For the second-round candidates, NIST will give the submission teams the opportunity to provide updated specifications and implementations to correct typos and implementation bugs. The deadline for these updates is September 27, 2019 11:59pm EDT.
NIST will review the proposed modifications and publish the accepted updates shortly afterwards. No major design changes will be accepted in this phase.

We estimate that the second round will last 12 months. NIST is planning to host the next Lightweight Cryptography Workshop on November 4-6, 2019 in Gaithersburg, MD. Please see the event page (https://csrc.nist.gov/Events/2019/lightweight-cryptography-workshop-2019) for further information regarding the workshop.

Questions may be directed to lightweight-crypto@nist.gov.

Thank you,
NIST lightweight cryptography team