

From: [Sonmez Turan, Meltem \(Assoc\)](#)
To: lwc-forum@list.nist.gov
Cc: [lightweight-crypto](#)
Subject: NIST Lightweight Cryptography Project - Second-round candidates
Date: Friday, August 30, 2019 2:23:43 PM

Dear subscribers of the NIST Lightweight Cryptography forum,

We would like to thank all submitters 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 more promising candidates.

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
SAEAS	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 selection process 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 design changes will be accepted in this phase.

The second round is expected to last 12 months. NIST will be hosting 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

