Open Discussion

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Standardization Procedure and Timeline

- Publication of the draft standards describing the Ascon family
  - Special Publication (SP) series rather than Federal Information Processing Standards (FIPS) (tentative decision)
  - One or more SP with multiple parts
  - Public comments period of 60 to 90 days

- Renaming possibility

- Tentative timeline: Fall 2023

Which AEAD variants should NIST standardize?

- Ascon-128 (primary)
- Alternatives:
  - Ascon-128a
  - Both Ascon-128 and Ascon-128a
  - Both Ascon-128 and Ascon-128a, with aligned round numbers (b=8)

	Variant	**Parameter sizes**
AEAD	**Ascon-128**	128-bit key/nonce/tag
	Ascon-128a	128-bit key/nonce/tag
	Ascon-80pq	160-bit key, 128-bit nonce/tag

Which hash functions/XOFs should NIST standardize?

- Ascon-Hash (primary)

- Alternatives:
  - Ascon-XOF (possibly along with tweaking IV)
  - Both Ascon-Hash and Ascon-XOF
  - For each option: Primary variant (b=12) or A-variant (b=8)?

	Variant	**Parameter sizes**
Hash	**Ascon-Hash**	256-bit digest
	Ascon-Hasha	256-bit digest
XOF	Ascon-XOF	Arbitrary length digest
	Ascon-XOFa	Arbitrary length digest

Standards Portfolio

- Ascon may be integrated into NIST’s portfolio of standards beyond the scope of the LWC call
- Additional functionalities: PRF, MAC, DRBG, etc.

Bit Ordering Convention

- Ascon currently follows SHA-2 convention: ***most*** significant bit in leftmost position
- SHA-3 convention: ***least*** significant bit in leftmost position

- Should Ascon be specified following SHA-3 convention?

Inputs and Outputs

- Larger key sizes
- 64-bit, 96-bit tag size
- Larger nonces
- Support for customization strings
- IVs may need to change to domain separate additional input/output sizes and functionalities

Thanks

- Ascon team
- Bart Mennink for the invited talk
- Presenters
- Sara Kerman for administrative support
- Conference support and AV teams

- Everyone who participated in the LWC standardization process

CONTACT US

lightweight-crypto@nist.gov

PUBLIC FORUM lwc-forum@list.nist.gov

GITHUB https://github.com/usnistgov/Lightweight-Cryptography-Benchmarking

WEBSITE https://csrc.nist.gov/Projects/lightweight-cryptography