Next Steps in NIST Lightweight Cryptography Standardization

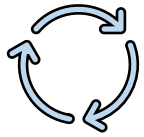
Meltem Sönmez Turan
NIST Lightweight Cryptography Team

September 27, 2023

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

MPTS 2023: NIST Workshop on Multi-party Threshold Schemes 2023

NIST Lightweight Cryptography Standardization Project



PROCESS

Public competition-like process with multiple rounds like AES, SHA3 and PQC standardization

GOAL

Develop new guidelines, recommendations and standards optimized for constrained devices

SCOPE

Authenticated Encryption and (optional) hashing for constrained software and hardware environments

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

Two workshops (2015, 2016) to get feedback on target applications, industry need, requirements, etc.

Publications:

- NISTIR 8114 *Report on Lightweight Cryptography*
- (White paper, retired) *Profiles for the Lightweight Cryptography Standardization Process*

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Submission Requirements and Evaluation Criteria

Deadline: February 2019

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

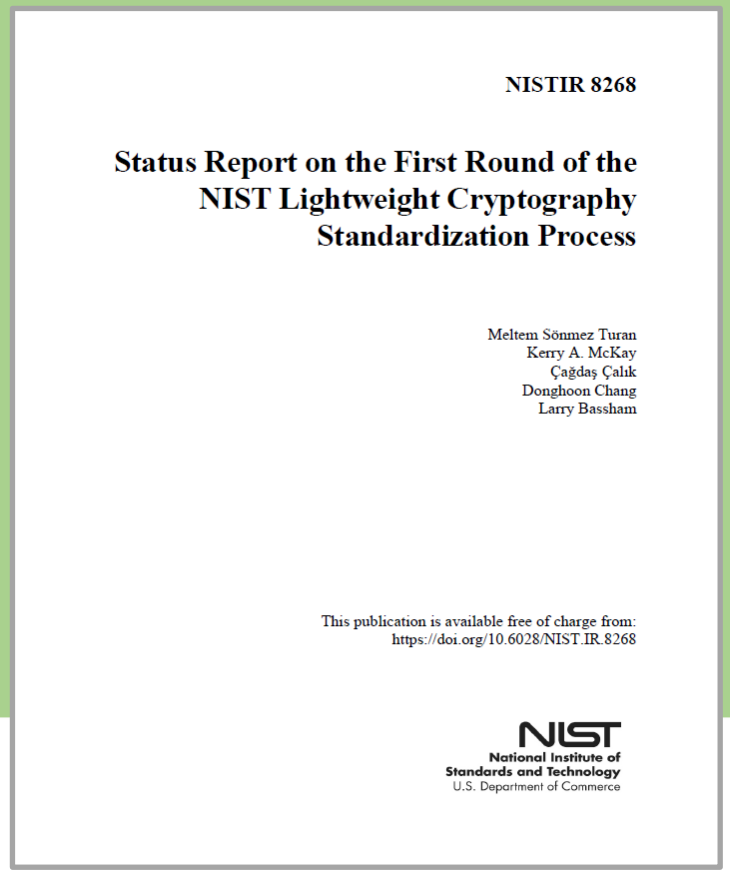
Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

56 First-round candidates

Evaluation only based on security

NIST IR 8268 explains how 32 candidates (out of 56) were selected to move forward to the second round.



NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8268

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

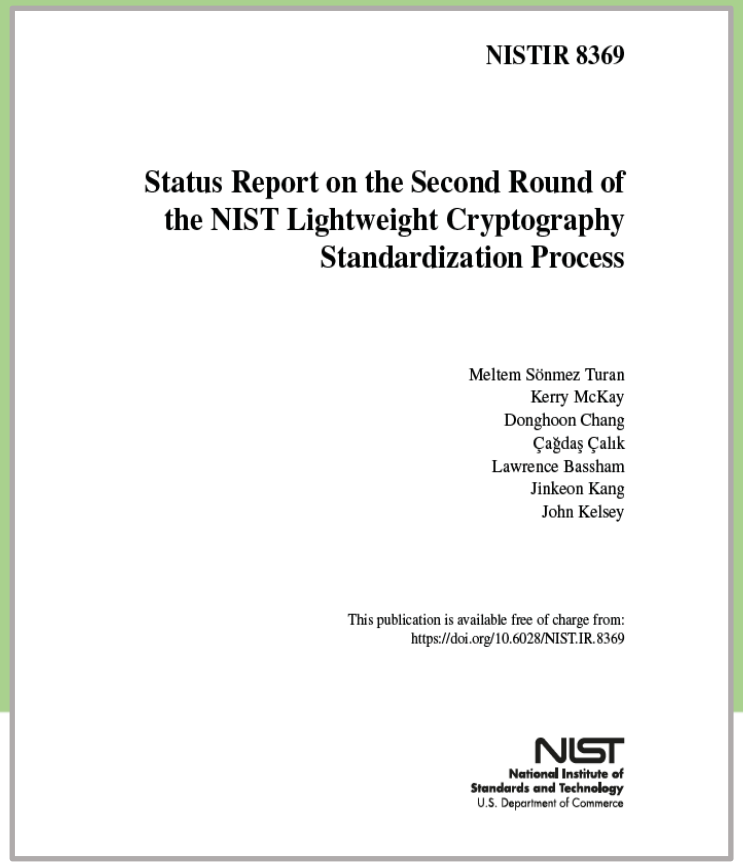
Round 2
(August 2019 – March 2021)

Final Round
(March 2021 – June 2023)

32 Second-round candidates

Two workshops (2019, 2020)

NIST IR 8369 explains how 10 finalists were selected to move forward to the final round.



NISTIR 8369

Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Çağdaş Çalık
Lawrence Bassham
Jinkeon Kang
John Kelsey

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8369

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Initial Phase
(July 2015 – August 2018)

Call for Candidates
(August 2018 – April 2019)

Round 1
(April 2019 – August 2019)

Round 2
(August 2019 – March 2021)

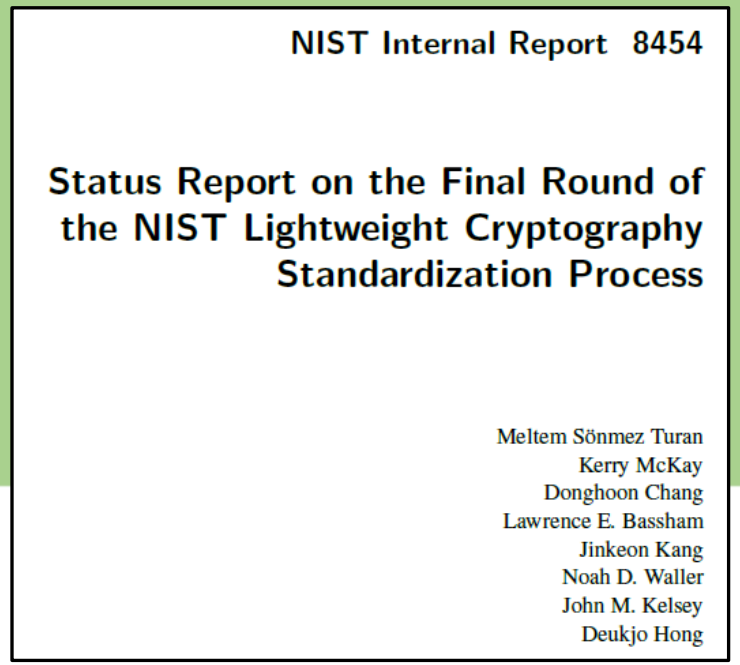
Final Round
(March 2021 – June 2023)

Ten finalists

- Ascon
- Elephant
- GIFT-COFB
- Grain-128AEAD
- ISAP
- Photon-Beetle
- Romulus
- Sparkle
- TinyJambu
- Xoodyak

Two workshops

NIST IR 8454 explains the selection of Ascon.



NIST Internal Report 8454

Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry McKay
Donghoon Chang
Lawrence E. Bassham
Jinkeon Kang
Noah D. Waller
John M. Kelsey
Deukjo Hong

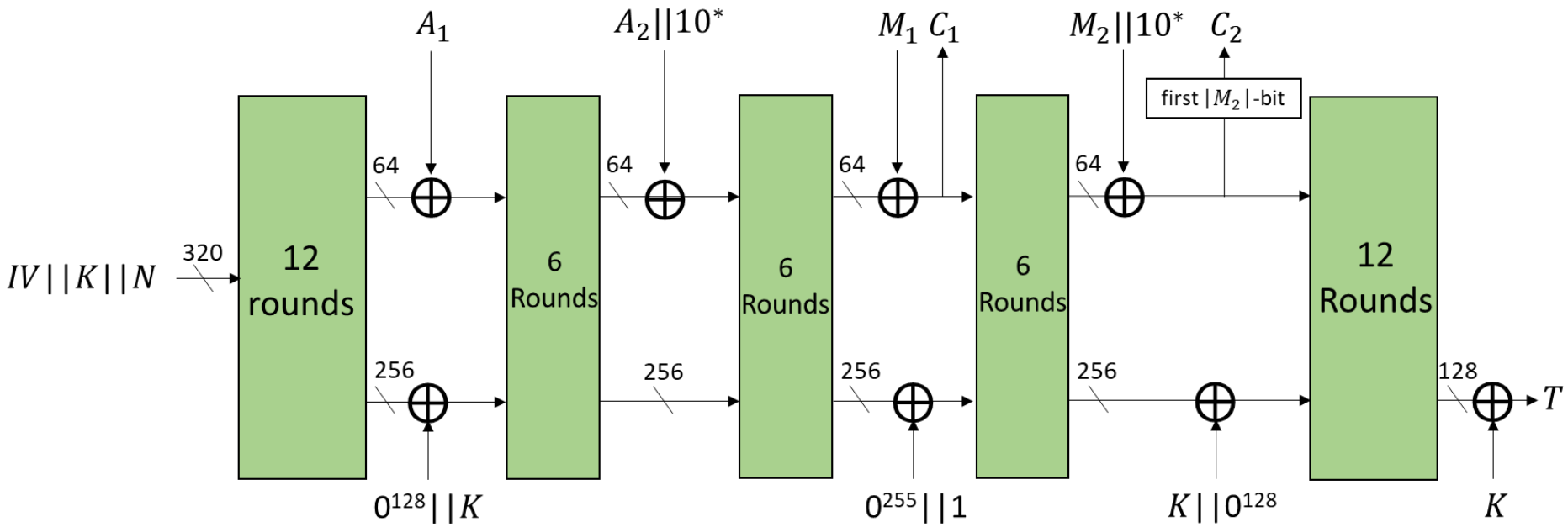
Selection of Ascon

In February 2023, NIST announced the Ascon family as the winner.

- High security margin, large number of third-party analysis
- Primary choice for the for lightweight applications in the final CAESAR portfolio
- No design tweaks
- Performance advantages over NIST standards (AES-GCM and SHA-2) in hardware and software
- Implementation and design flexibility
- Mode-level protection mechanism against leakage and lower additional cost for protected implementations
- Support for additional functionalities XOF, dedicated MAC, in addition to Hash

ASCON

- AEAD and hashing scheme (fixed or variable output length)
- Main component: 320-bit permutation instantiated with different constants and number of rounds for different variants
- AEAD: MonkeyDuplex mode with keyed initialization and finalization
- Hash: Sponge construction



The primary AEAD variant of Ascon family

VARIANTS

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

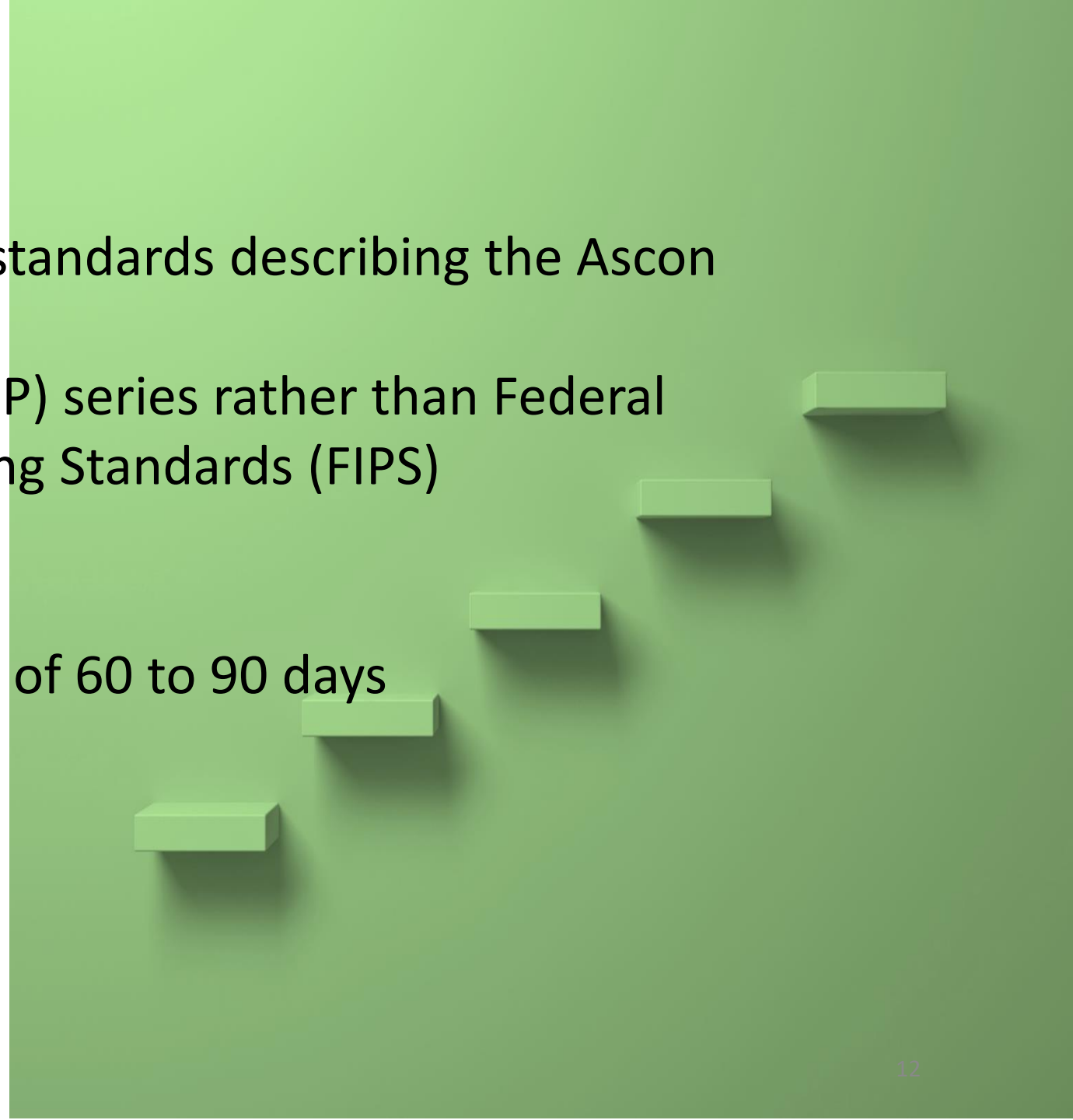
Current tentative decisions:

- Either Ascon-128 or both Ascon-128 and Ascon-128a
- Do not include Ascon-80pq
- XOF standardization instead of hash functions

NEXT STEPS

- Publication of the draft standards describing the Ascon family (later in 2023)
  - Special Publication (SP) series rather than Federal Information Processing Standards (FIPS) (tentative decision)

- Public comments period of 60 to 90 days



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

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