Security Conference 2022

Towards a New Lightweight Cryptography Standard

Meltem Sonmez Turan

October 5, 2022

Agenda

- Overview of the standardization process
- Evaluation of the finalists
- Next steps

Lightweight Cryptography

CONSTRAINED DEVICES

e.g., RFID tags, sensors, IoT devices

NEW APPLICATIONS

e.g., home automation, healthcare, smart city

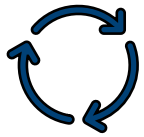
PRIVATE INFORMATION

e.g., location, health data, usage patterns

LACK OF CRYPTOGRAPHY STANDARDS

NIST crypto standards are optimized for general-purpose computers

NIST Lightweight Cryptography Standardization Process



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.

In August 2018, NIST published the 'Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process'.

Submission deadline: February 2019

Requirements

AEAD

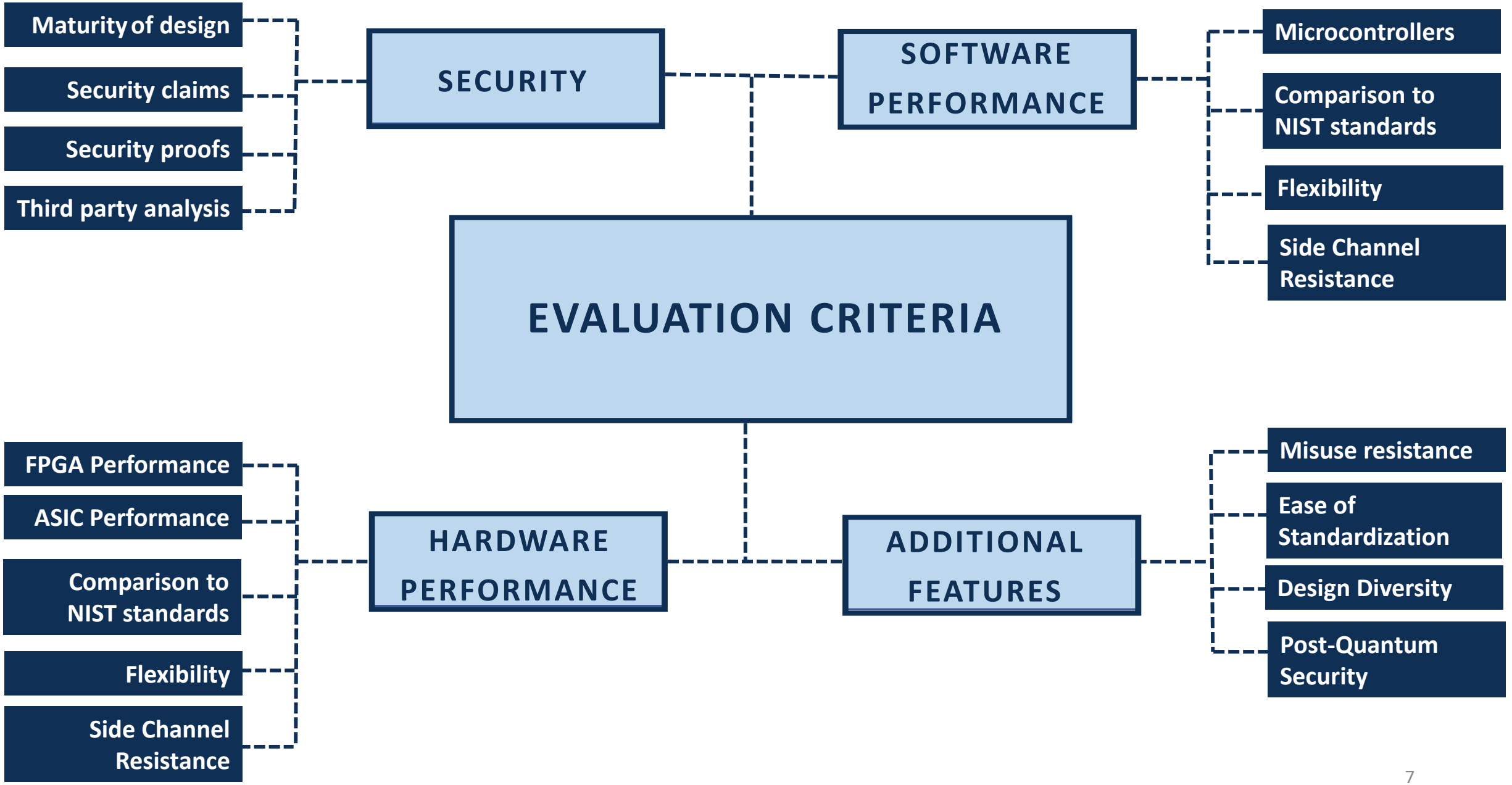
- Confidentiality of the plaintexts (under adaptive chosen-plaintext attacks) + Integrity of the ciphertexts (under adaptive forgery attempts)
- At least 128-bit key, at least 2^{112} computation for attacks (nonce is assumed to be unique under the same key)
- Family of (at most 10) algorithms
  - One **primary member** with key ≥ 128 bits, nonce ≥ 96 bits and tag ≥ 64 bits
  - Limits on the input sizes for the primary member at least 2^{50}-1 bytes

Hash

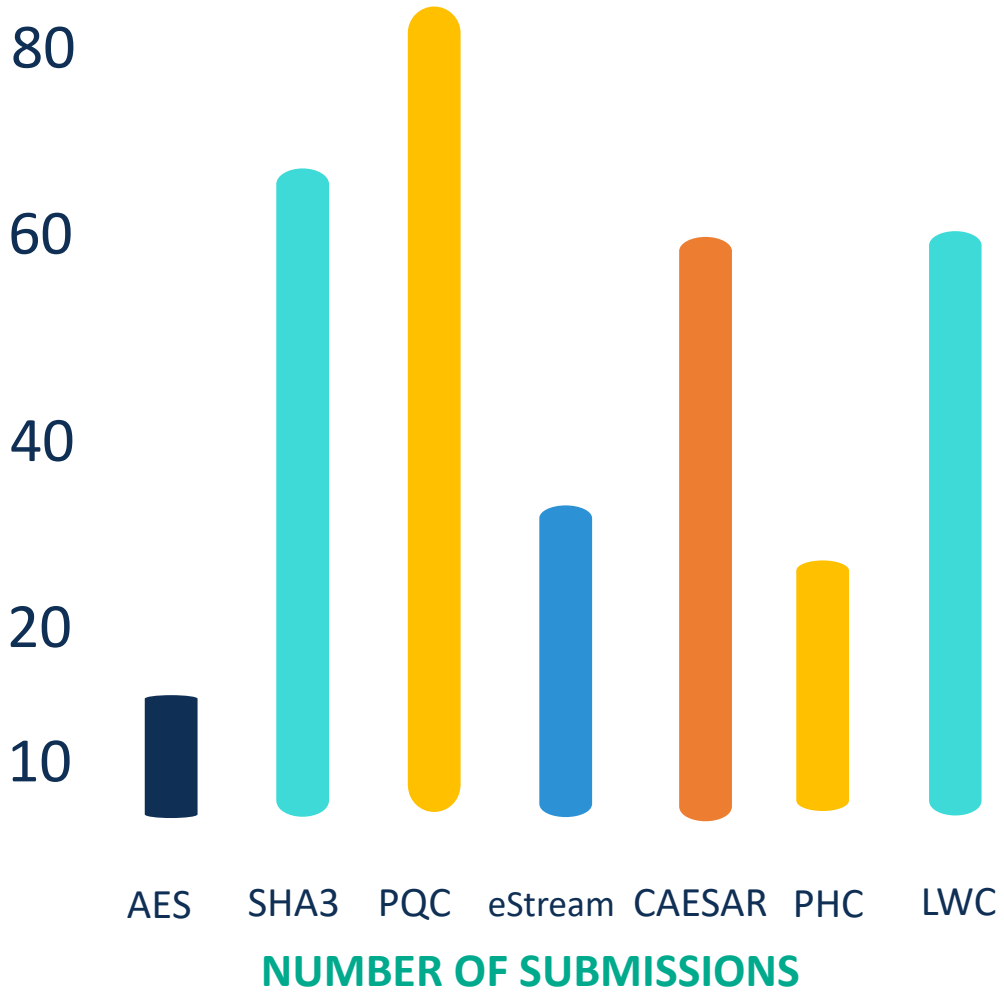
- Computationally infeasible to find a collision or a (second) preimage. Resistance to length extension attacks. (Attacks requiring at least 2^{112} computations)
- Digest size at least 256 bits
- Family of (at most 10) algorithms
  - One **primary member** has a hash size of 256 bits.
  - Limits on the input sizes for the primary member at least 250-1 bytes
- Common design components with the AEAD

Design and implementation

- Perform significantly better in constrained environments (HW and SW platforms) compared to NIST standards, efficient for short messages, implementations that are easy to protect against side channel attacks, and fault attacks


EVALUATION CRITERIA
SECURITY
Maturity of design
Security claims
Security proofs
Third party analysis
SOFTWARE PERFORMANCE
Microcontrollers
Comparison to NIST standards
Flexibility
Side Channel Resistance
HARDWARE PERFORMANCE
FPGA Performance
ASIC Performance
Comparison to NIST standards
Flexibility
Side Channel Resistance
ADDITIONAL FEATURES
Misuse resistance
Ease of Standardization
Design Diversity
Post-Quantum Security

Submissions



FROM 25 COUNTRIES

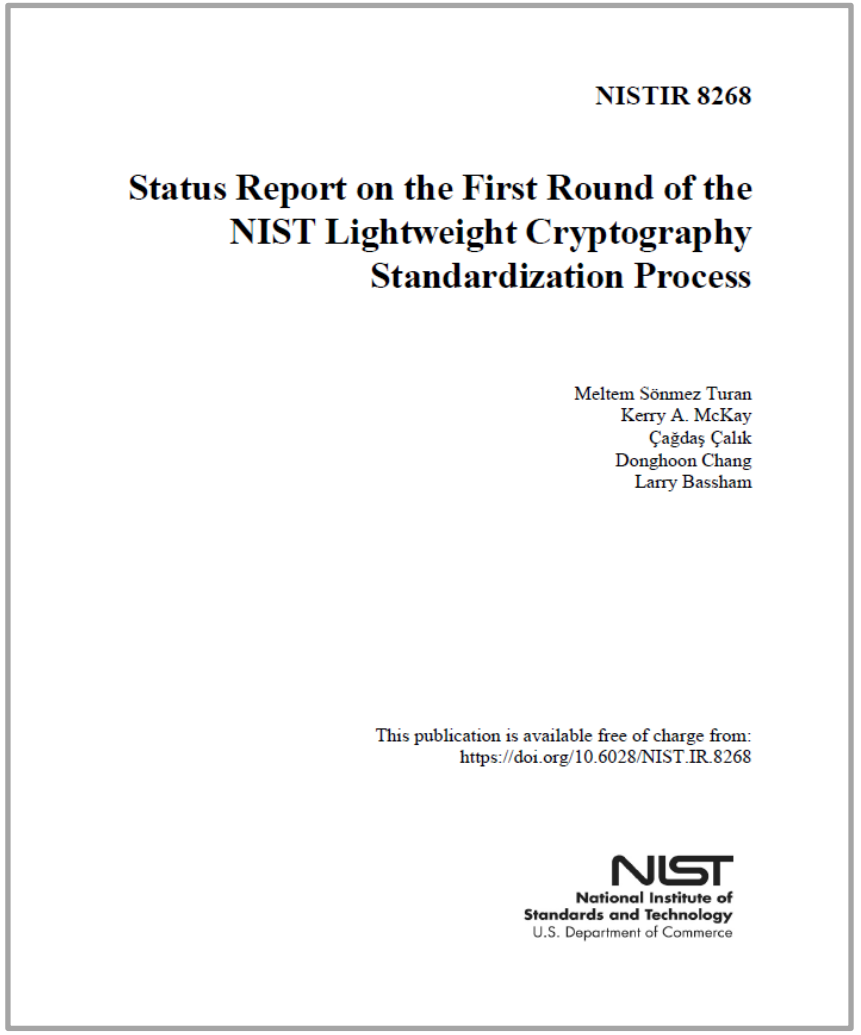
Round 1

Time period: April – August 2019

Evaluation criteria: Security

- e.g., distinguishing attacks, practical tag forgeries, domain separation issues, new designs with no third-party analysis etc.

56 First-round Candidates → 32 Second-round Candidates



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

Second Round Candidates

- ACE
- ASCON
- COMET
- DryGascon
- Elephant
- ESTATE
- ForkAE
- GIFT-COFB
- Gimli
- Grain128aead
- HyENA
- ISAP
- KNOT
- LOTUS-LOCUS
- mixFeed
- ORANGE
- Oribatida
- Photon-Beetle
- Pyjamask
- Romulus
- SAEAES
- Saturnin
- Skinny-AEAD
- Sparkle
- SPIX
- SpoC
- Spook
- Subterranean
- Sundae-GIFT
- TinyJambu
- Wage
- Xoodyak

Software Benchmarking

Microcontroller benchmarking by NIST LWC Team

Devices:
- 8-bit AVR
- 32-bit ARM Cortex M0+, M4
- MIPS32 M4K
- Tensilica L106

Metrics:
- Code size
- Speed

Microcontroller benchmarking by Renner et al.

Devices:
- 8-bit AVR
- 32-bit ARM Cortex M3, M7
- Tensilica Xtensa LX6
- RISC-V

Metrics:
- Size
- RAM usage

Microcontroller benchmarking by Weatherly

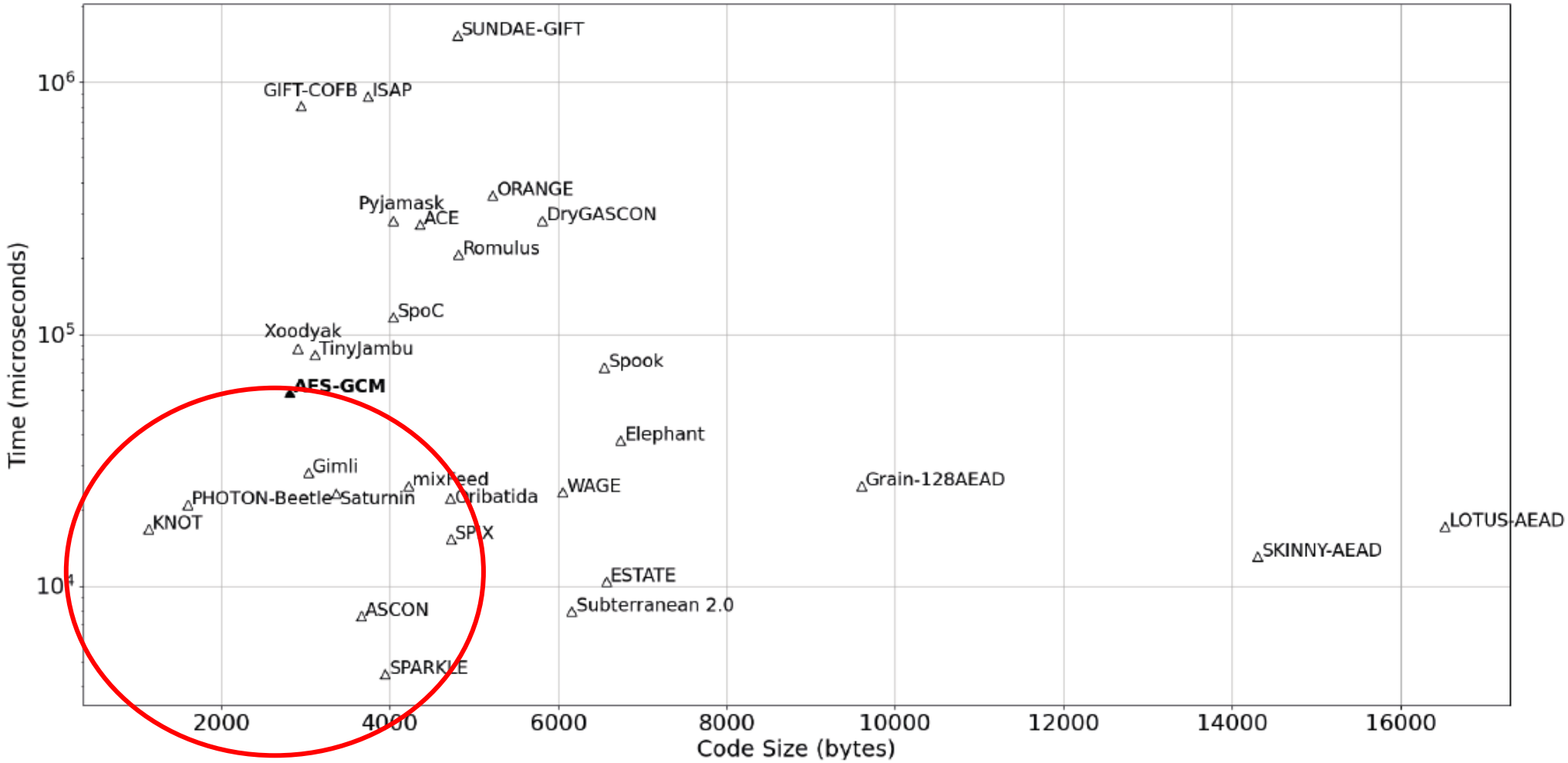
Devices:
- AVR
- ARM Cortex-M3
- Tensilica Xtensa LX6

Metrics:
- Speed

eBACS (ECRYPT Benchmarking of Cryptographic Systems) by Lange and Bernstein

Devices:
- Many systems covering ARM, AMD, Intel, PPC, RISC V, and MIPS architectures

Metrics:
- Speed



Code size vs. speed results of the smallest primary AEAD variants - 16-byte message and 16-byte AD on ATmega328P

Software Benchmarking

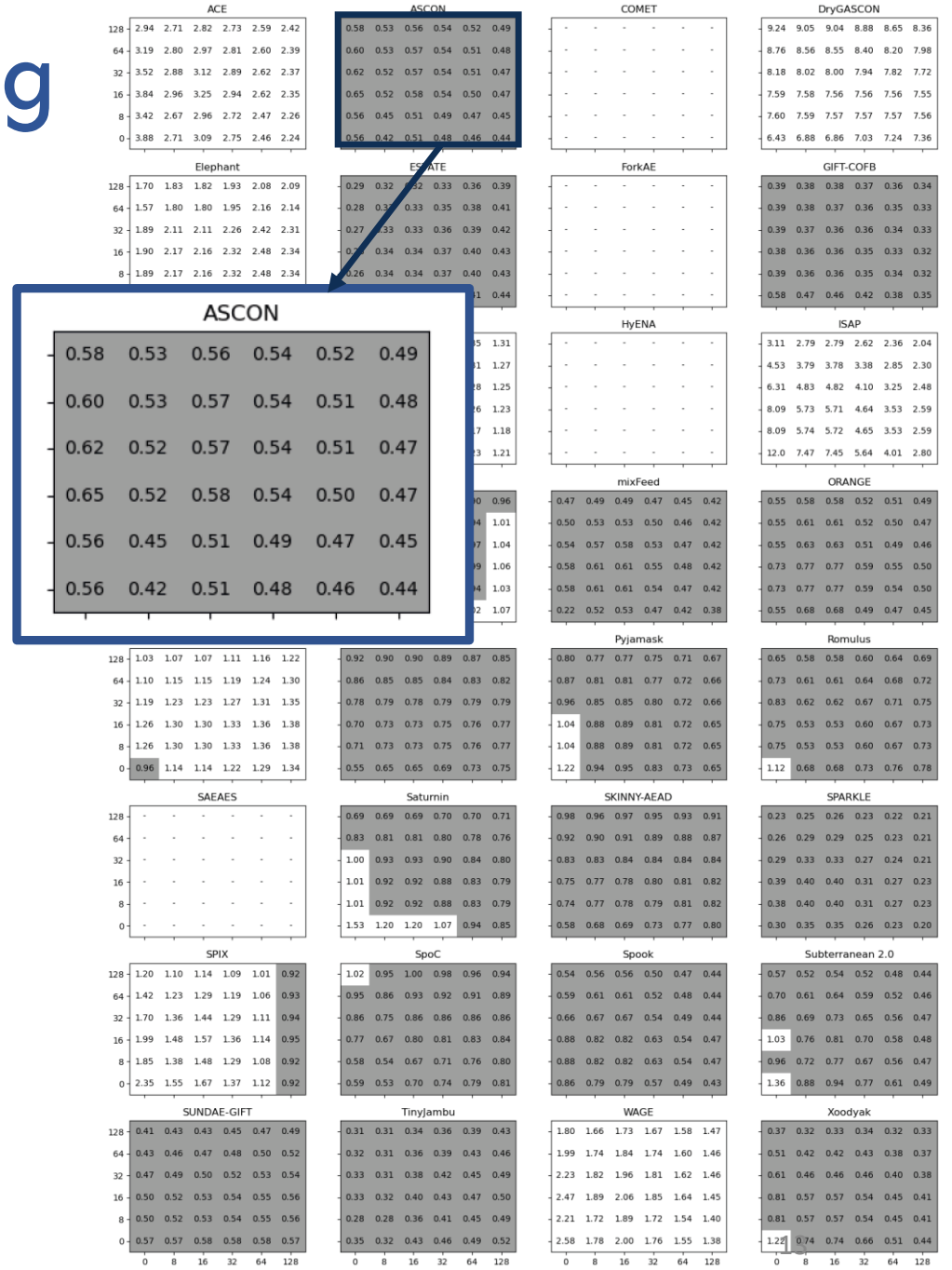
Relative timings for each candidate are shown by a matrix of values, where

- rows = message lengths (0 bytes – 128 bytes),
- columns = AD lengths (0 bytes – 128 bytes).

$$\textbf{Metric} = \frac{\text{Execution time of the candidate}}{\text{Execution time of AES–GCM}}$$

Result:

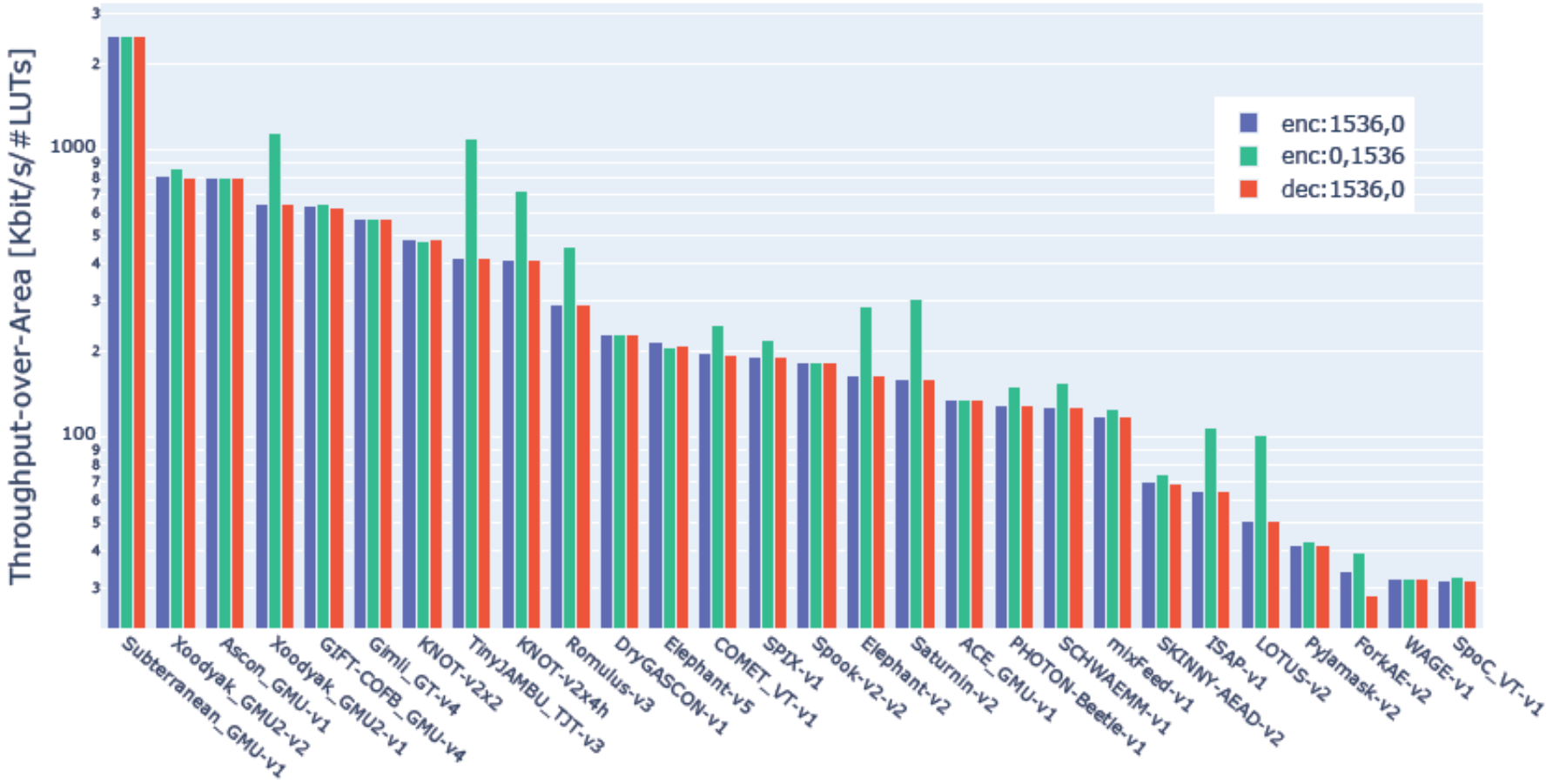
Ascon, Estate, Gimli, Knot, Lotus-AEAD, mixFeed, Orange, Photon-Beetle, Pyjamask, Romulus, Saturnin, Skinny-AEAD, Sparkle, Spoc, Spook, Subterranean, SUNDAE-GIFT, TinyJambu, Xoodyak perform better than AES-GCM on ATmega328P.



Round 2 Hardware Benchmarking

Initiative	*Platforms*	*Metrics*
GMU CERG group	Xilinx Artix-7 Intel Cyclone 10 LP Lattice Semiconductor ECP5	Resource utilization (LUT or LE, flip-flops) Maximum clock frequency (MHz) Throughput (Mbits/s) Energy per bit (nJ/bit)
Khairallah et al.	TSMC 65nm FDSOI 28nm	Area (μm^2 and GE) Clock period (ns) Power (mW) Energy (mJ)
Aagaard and Zidarič	ST Micro 65nm TSMC 65nm ST Micro 90nm TSMC 90nm ARM/IBM 130nm	Throughput (bits per cycle) Area (GE) Energy (nJ) Area×Energy (GE×nJ) Clock Speed (GHz)

Round 2 Hardware Benchmarking



Throughput-over-Area for Authenticated Encryption and Decryption of 1536-byte messages at 75MHz by GMU

Round 2

Time period: Aug. 2019 – March 2021

Evaluation criteria: security analysis, performance benchmarks

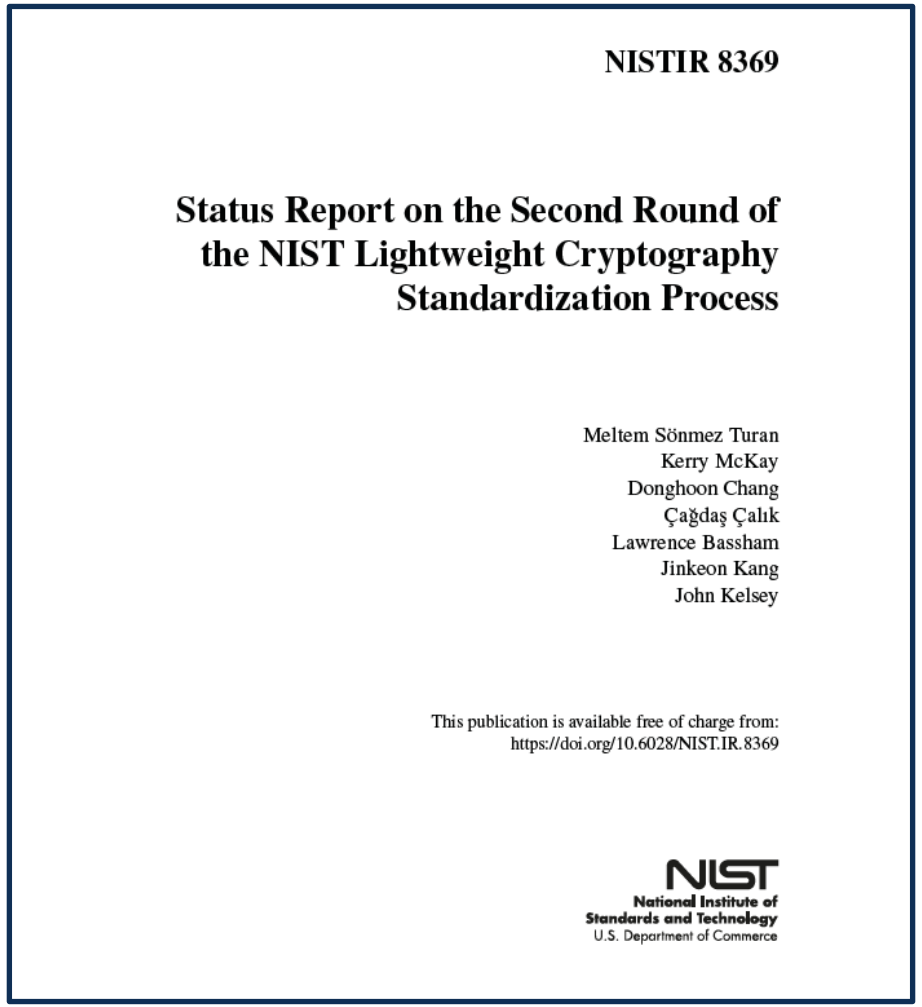
Two workshops

- Nov. 2019 – Third LWC Workshop
- Oct. 2020 – Fourth LWC Workshop (virtual)

56 first-round candidates → 32 second-round candidates → 10 finalists

March 2021, NIST announced ten finalists.

ASCON	**Elephant**	**GIFT-COFB**	**Grain-128aead**	**ISAP**
Photon-Beetle	**Romulus**	**Sparkle**	**TinyJambu**	**Xoodyak**



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

Round 3

Time period: March 2021 – December 2022 (tentative)

Evaluation criteria: Security, performance benchmark, side channel analysis, and additional features.

Decision relies on publicly available analysis and benchmarking results. Use of **lwc-forum** is highly encouraged.

Workshop

- May 2022 – Fifth LWC Workshop (virtual)

Challenges:

- Assigning weights for different criteria: Different security claims, different functionality, attacks with different complexities
- Fair evaluation: Not all algorithms get the same public attention.

Variants

Finalist	# Variants	Key size (bits)	Nonce size (bits)	Tag size (bits)	Digest size (bits)
Ascon	2 aead 2 hash	128 --	128 --	128 --	-- 256
Elephant	3 aead	128	96	64-128	--
GIFT-COFB	1 aead	128	128	128	--
Grain-128aead	1 aead	128	96	64	--
ISAP	4 aead	128	128	128	--
PHOTON-Beetle	2 aead 1 hash	128 --	128 --	128 --	-- 256
Romulus	3 aead 1 hash	128 --	128 --	128 --	-- 256
Sparkle	4 aead 2 hash	128-256 --	128-256 --	128-256 --	-- 256-384
TinyJambu	3 aead	128-256	96	64	
Xoodyak	1 aead 1 hash	128 --	128 --	128 --	-- 256

Underlying Components - Finalists

AEAD-only

Permutation

- Elephant
- ISAP

Block Cipher

- GIFT-COFB
- TinyJAMBU

Stream cipher

- Grain-128AEAD

AEAD and Hashing

Permutation

- ASCON
- PHOTON-Beetle
- SPARKLE
- Xoodyak

Tweakable block cipher

- Romulus

Modes of Operation - Finalists

Sequential

Classical/modified Sponge with Public Permutation
ASCON, Xoodyak, PHOTON-Beetle, SPARKLE

(T)BC-based Feedback with Rate 1
GIFT-COFB, Romulus

Enc-then-Mac
ISAP

Classical Sponge with Secret Permutation
TinyJAMBU

Stream Cipher Based
Grain-128AEAD

Parallel

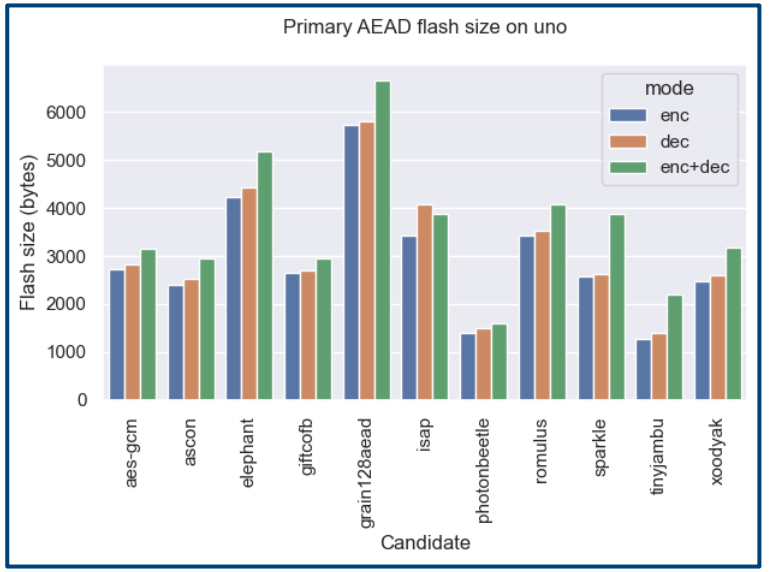
Enc-then-Mac
Elephant

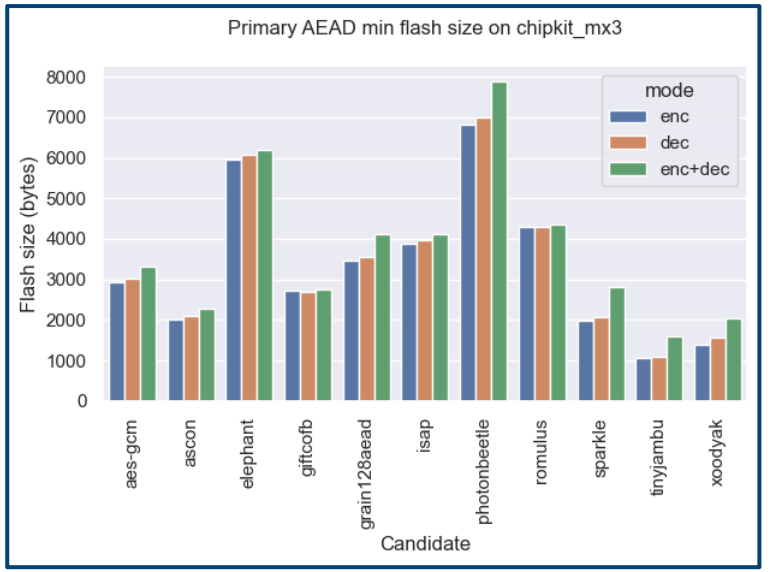
* For primary variants

Software Benchmarking - Finalists

Ongoing software benchmarking by NIST team, partial results are on project GitHub page.

No	Finalists	Submission Package						Additional	Total incl. Additional
		Total	#AEAD	#Hash	#(AEAD+Hash)	#AEAD Primary	#Hash Primary		
1	ASCON	85	31	36	18	11	9	61	146
2	Elephant	3	3			1			3
3	GIFT-COFB	1	1			1		6	7
4	Grain-128AEAD	5	5			5			5
5	ISAP	22	18		4	5		4	26
6	PHOTON-beetle	40	16	8	16	8	8	6	46
7	Romulus	21	11	4	6	5	4	34	55
8	SPARKLE	32	21	11		6	6	6	38
9	TinyJambu	6	6			2			6
10	Xoodyak	4	2	2		2	2		4
	Total	219	114	61	44	46	29	117	336





Timeline

Early stage 2015-2018	2019	2020 – 2022	Late 2022 -- …
First workshop Second workshop NISTIR 8114 Profiles Call	Submissions due Beginning of Round 1 NISTIR 8268 Beginning of Round 2 Third workshop	Fourth workshop Announcement of the finalists Beginning of Round 3 NISTIR 8369 Fifth workshop	*Announcement of the winner(s)* *Beginning of standardization*

Next Steps

- Selection of the winner(s) and the publication of the status report
- Standardization is expected to start in 2023.

Thanks!

CONTACT NIST TEAM
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