

Update on the NIST Lightweight Cryptography Standardization Process

Meltem Sonmez Turan

NIST Lightweight Cryptography Workshop, May 9, 2022

Agenda

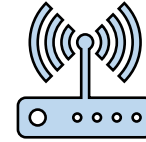
- Overview of the standardization process
- Selecting the finalist
- Evaluating the finalists
- Next steps

Motivation



CONSTRAINED DEVICES

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



NEW APPLICATIONS

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



PRIVATE INFORMATION

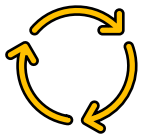
e.g., location, health data



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

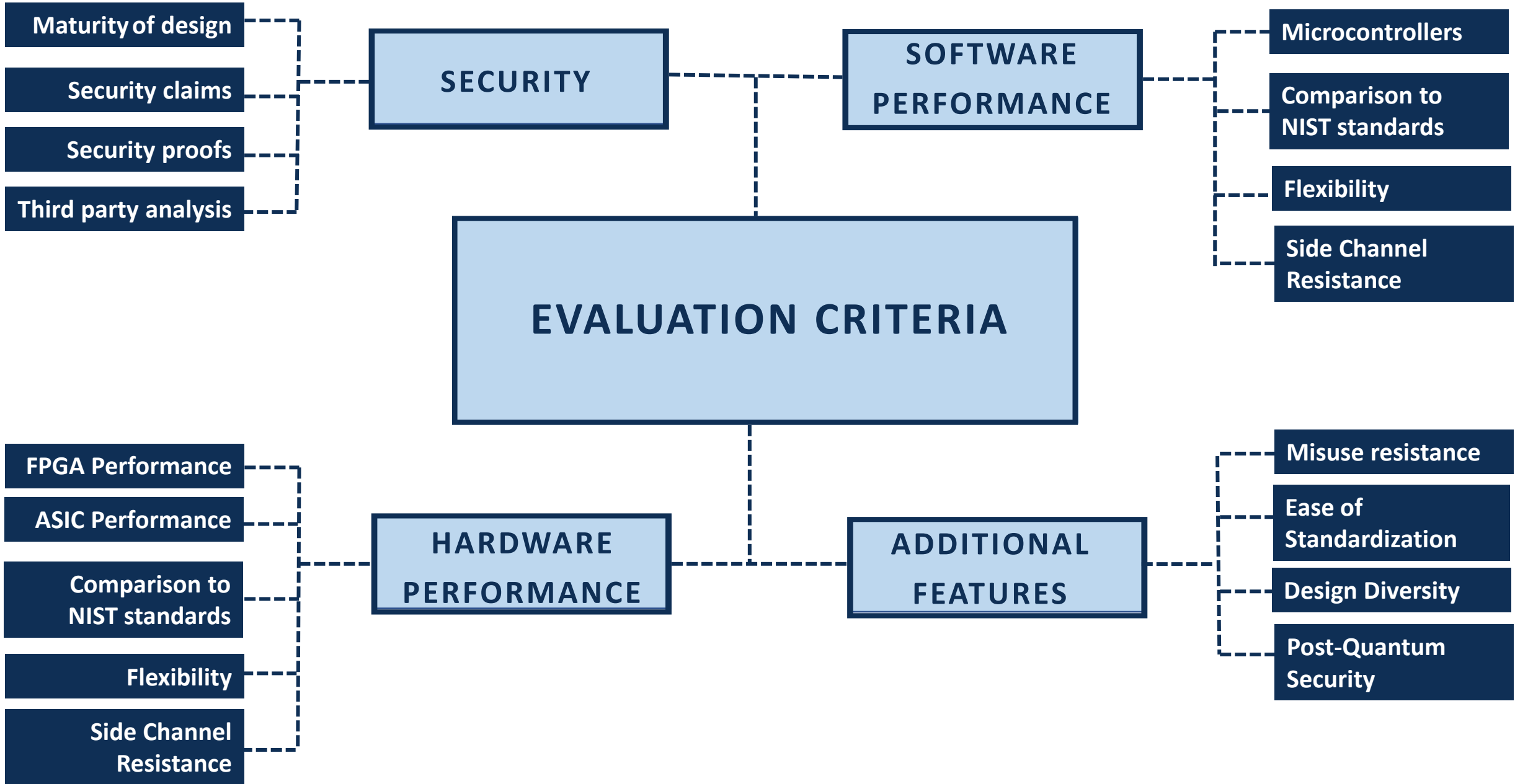
- Confidentiality of the plaintexts (under adaptive chosen-plaintext attacks) + Integrity of the ciphertexts (under adaptive forgery attempts)
- At least 128-bit key, at least 2^{112} computation for attacks (nonce is assumed to be unique under the same key)
- Family of (at most 10) algorithms
 - One **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

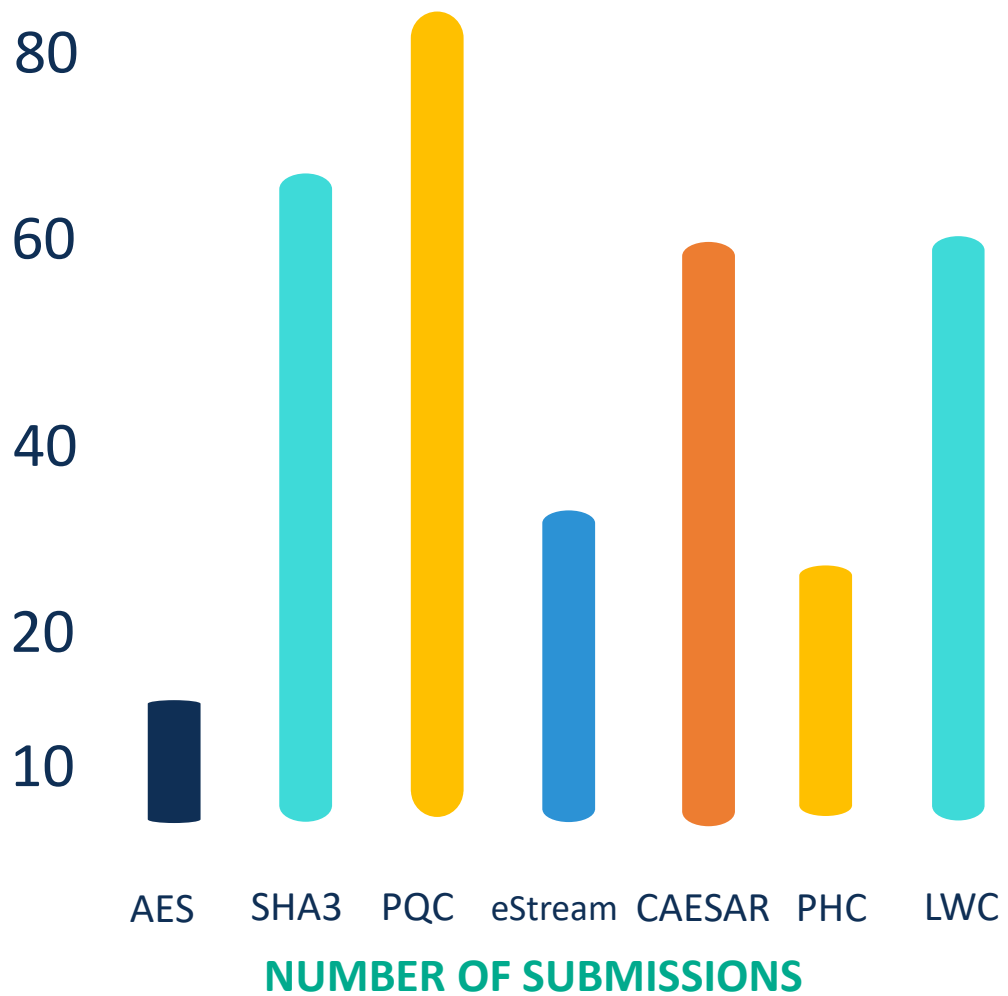
- Computationally infeasible to find a collision or a (second) preimage. Resistance to length extension attacks. (Attacks requiring at least 2^{112} computations)
- Digest size at least 256 bits
- Family of (at most 10) algorithms
 - One **primary member** has a hash size of 256 bits.
 - Limits on the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

Design and implementation

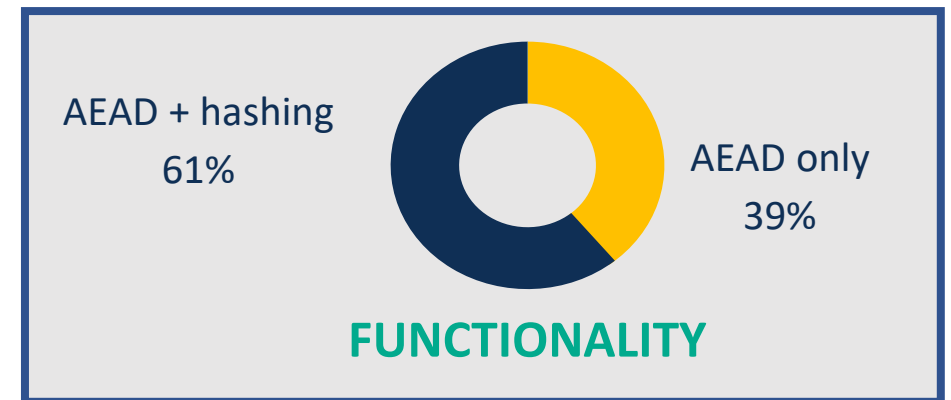
- Perform significantly better in constrained environments (HW and SW platforms) compared to NIST standards, efficient for short messages, implementations that are easy to protect against side channel attacks, and fault attacks



Submissions



FROM 25 COUNTRIES



Round 1



Around 5 months (from April to August 2019).

Evaluation of the candidates were done based on their security

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

32 Candidates (out of 56) are 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

Second-Round Candidates

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

Underlying Components

AEAD-only

Permutation

- Elephant
- ISAP
- Oribatida
- SPIX
- Spoc
- Spook
- Wage

Block Cipher

- COMET
- GIFT-COFB
- HyENA
- mixFeed
- Pyjamask
- SAEAEs
- SUNDAE-GIFT
- TinyJAMBU

Tweakable block cipher

- ESTATE
- ForkAE
- LOTUS-AEAD & LOCUS-AEAD
- Romulus
- Spook

Stream cipher

- Grain-128AEAD

AEAD and Hashing

Permutation

- ACE
- ASCON
- DryGASCON
- Gimli
- KNOT
- ORANGE
- PHOTON-Beetle
- SPARKLE
- Subterranean 2.0
- Xoodyak

Block Cipher

- Saturnin

Tweakable block cipher

- Skinny-AEAD & Skinny-Hash

Modes of Operation

Sequential

Classical Sponge with Public Permutation
ACE, ASCON, DryGASCON, Gimli, KNOT, Spix, Spook,
Subterranean 2.0, WAGE, Xoodyak

Modified Sponge with Public Permutation
ORANGE, Oribatida, PHOTON-Beetle, SPARKLE, SpoC

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

Classical Sponge with Secret Permutation
SAEAES, TinyJAMBU

Enc-then-Mac
ISAP, Saturnin

Mac-then-Enc
ESTATE, SUNDAE-GIFT

Stream Cipher Based
Grain-128AEAD

Parallel

ForkAE

LOTUS-AEAD & LOCUS-AEAD

OCB3-based
SKINNY-AEAD

OCB3-based
Pyjamask

Enc-then-Mac
Elephant

* For primary variants

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

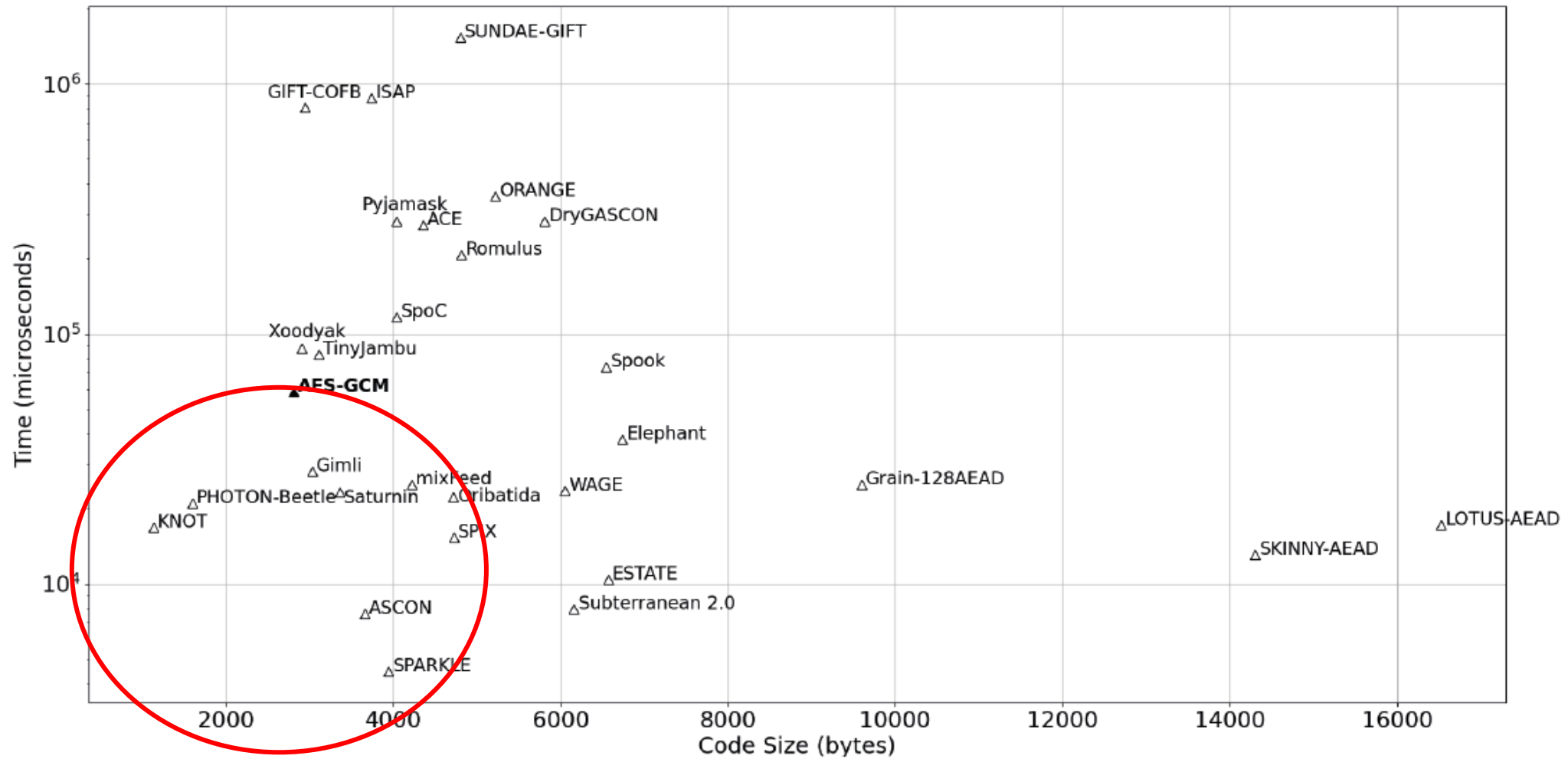
eBACS (ECRYPT Benchmarking of Cryptographic Systems) by Lange and Bernstein

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

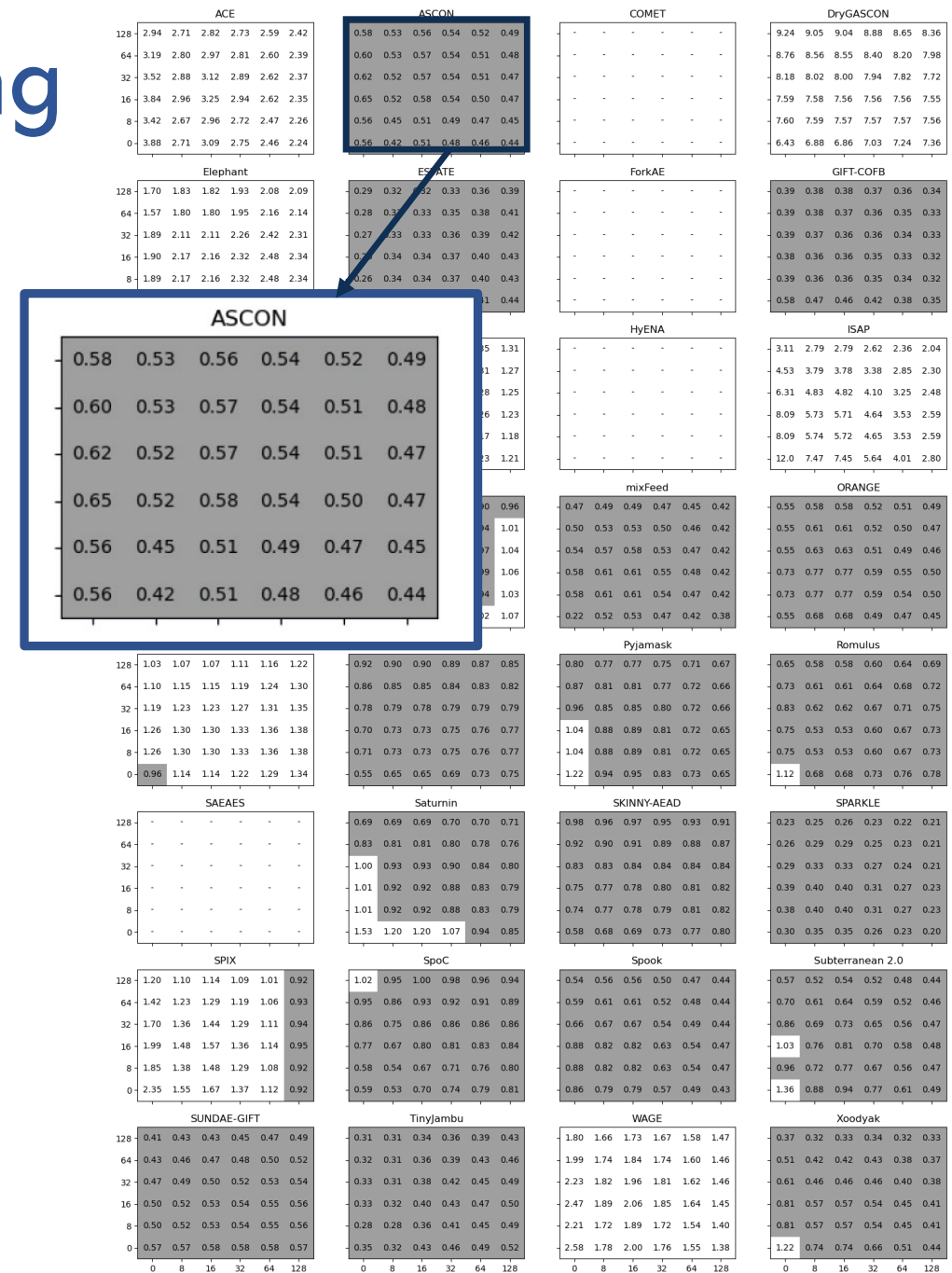
Relative timings for each candidate are shown by a matrix of values, where

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

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

Result:

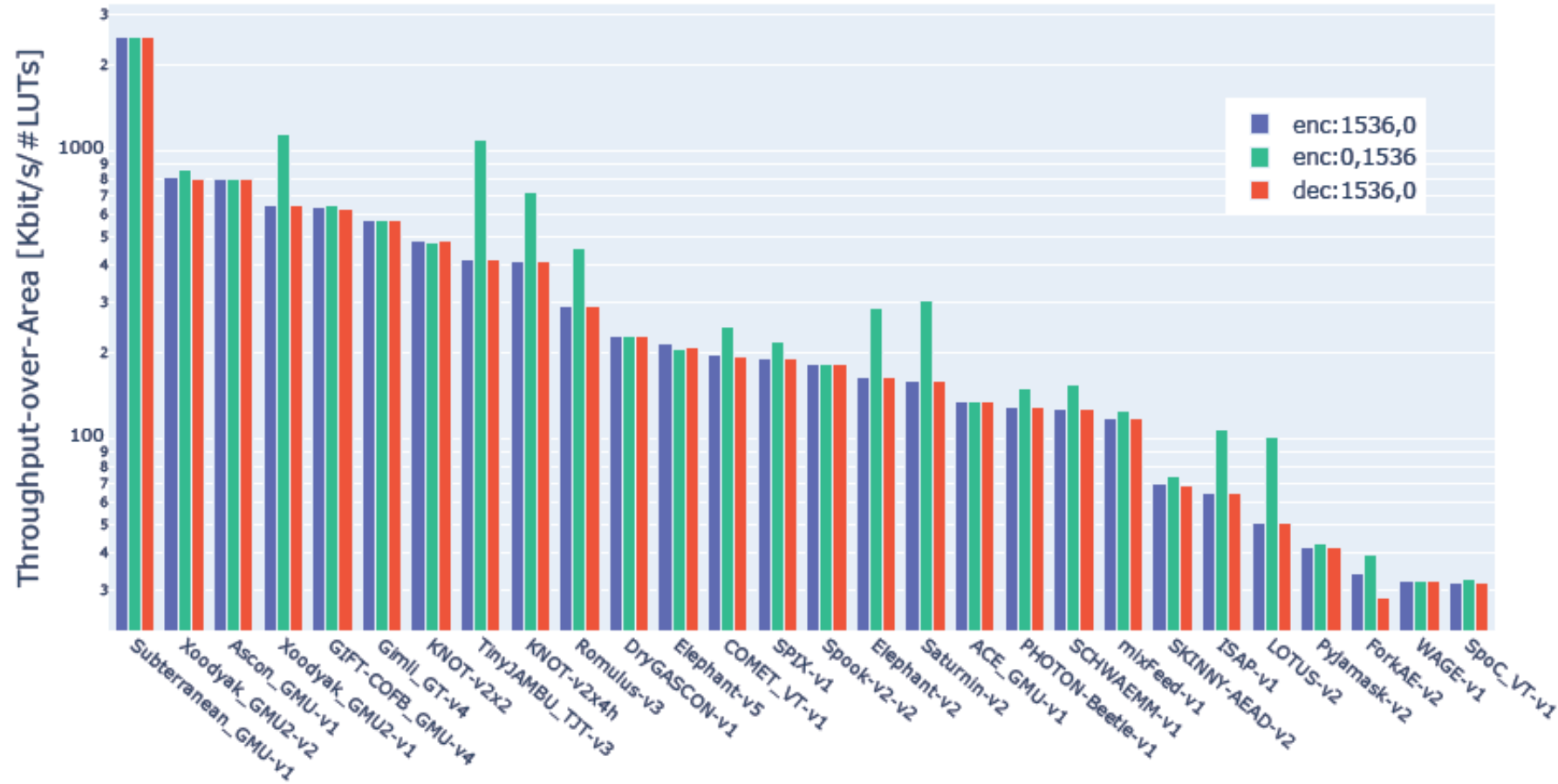
Ascon, Estate, Gimli, Knot, Lotus-AEAD, mixFeed, Orange, Photon-Beetle, Pyjamask, Romulus, Saturnin, Skinny-AEAD, Sparkle, Spoc, Spook, Subterranean, SUNDIAE-GIFT, TinyJambu, Xoodoo perform better than AES-GCM on ATmega328P.



Round 2 Hardware Benchmarking

<i>Initiative</i>	<i>Platforms</i>	<i>Metrics</i>
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 \times Energy (GE \times nJ) Clock Speed (GHz)

Round 2 Hardware Benchmarking



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

Status Updates

Towards the end of Round 2, NIST requested *optional status updates* from the submission teams on

- new proofs/arguments supporting the security claims,
- new software and hardware implementations
- new third-party analysis and its implications,
- platforms and metrics in which the candidate performs better than current NIST standards,
- target applications and use cases for which the candidate is optimized,
- planned tweak proposals, if submission accepted as a finalist, and
- any other relevant information.

NIST received 27 status updates.

Selecting the Finalists

Evaluation for 20 months (Aug. 2019 – March 2021), based on publicly available security analysis, and performance benchmarks

Two workshops

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

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>

Final Round Tweaks



Ascon: new family members, hash function **ASCON-Hasha** and **ASCON-Xofa**

Elephant: mode update to switch from the Wegman-Carter-Shoup MAC to a protected counter sum MAC to achieve authenticity under nonce-reuse.

Grain-128aead: a new cipher initialization and update function

ISAP: update on the ordering of the recommendations

Romulus: new family members: **Romulus-H** hash function and **Romulus-T** leakage-resilient AEAD mode. Removed non-primary members Romulus-N and Romulus-M. Skinny-128-384 reduced to 40 rounds instead of 56.

Sparkle: the primary variant has changed from SCHWAEMM192-192 to SCHWAEMM256-128

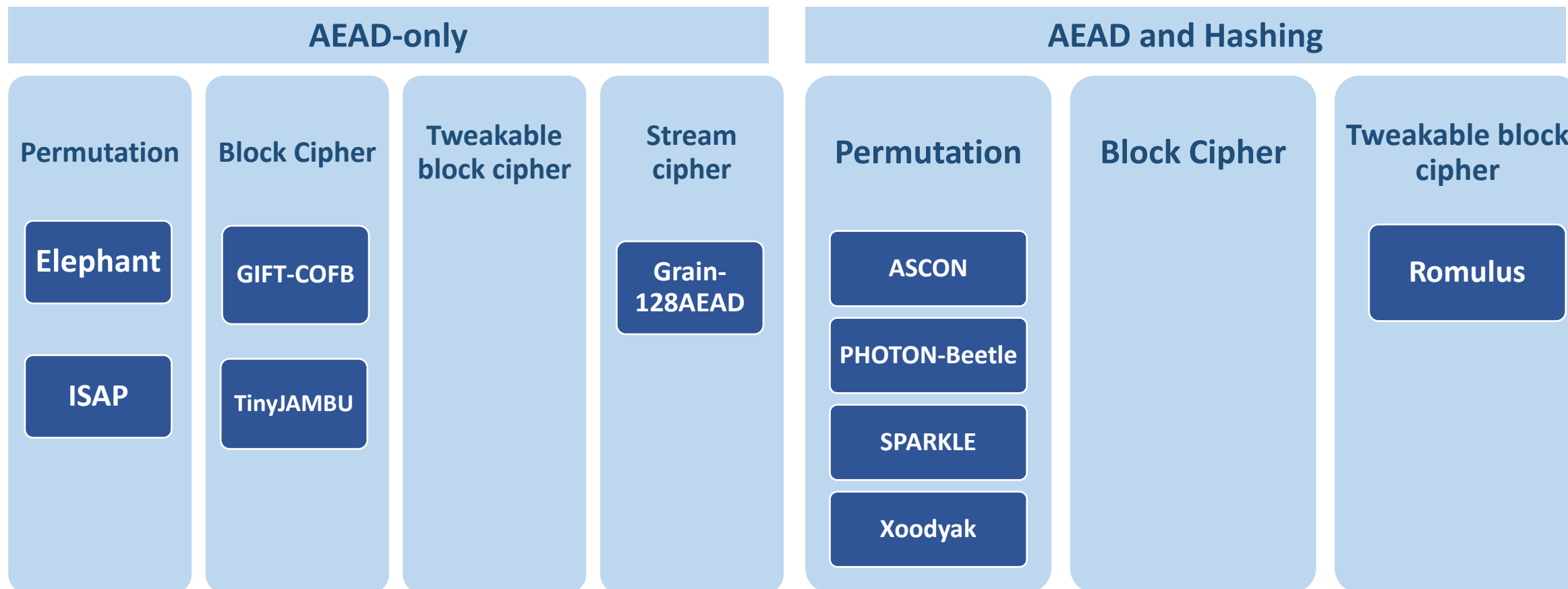
TinyJambu: Number of rounds increased from 384 to 640 to process AD and nonce

Xoodyak: Key and nonce processed in the same call to have efficiency for short messages.

Recommended Variants

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

Underlying Components - Finalists



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

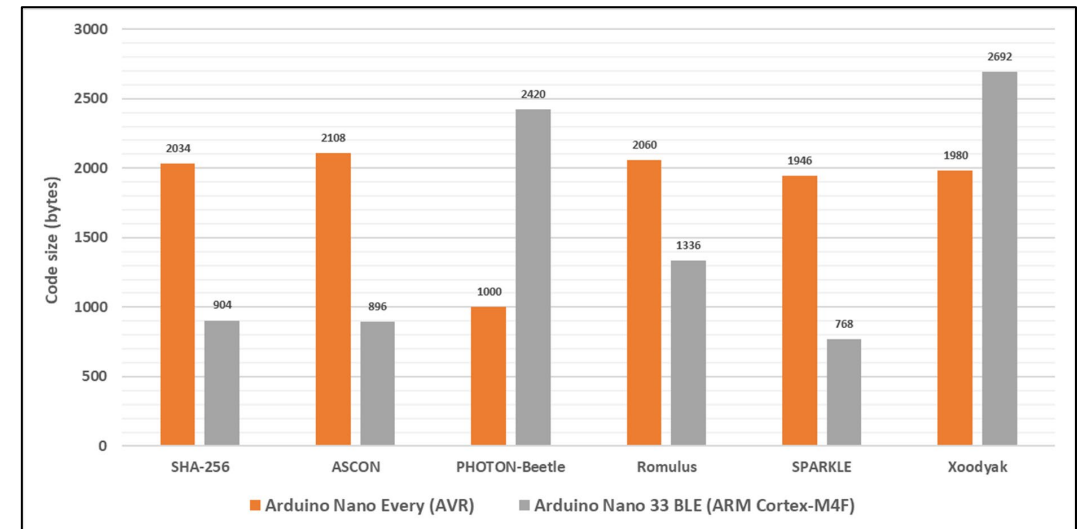
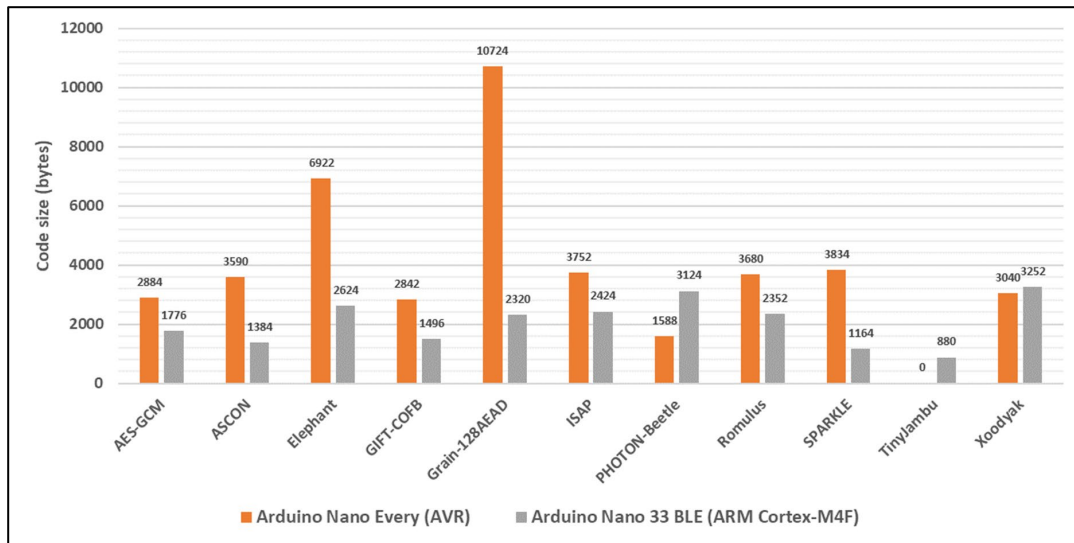
Elephant

Software Benchmarking - Finalists



- Ongoing SW benchmarking by NIST team
- Results will be published in the 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



Evaluation of the Finalists



In the final round, evaluation will also include side channel analysis of the finalists.

- New initiative by the GMU/CERG team

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




Challenges:

- **Assigning weights for different criteria:** Different security claims, different functionality, attacks with different complexities
- **Limited resources:** Not all algorithms get the same attention.

Timeline

Early stage 2015-2018	2019	2020 – 2021	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 <i>Announcement of the winner(s)</i> <i>Beginning of standardization</i>

Next Steps

-  Continue evaluating the finalists. Status updates (optional) from the finalists expected deadline early Fall 2022.
-  Selection of the winner(s) and the publication of the status report
-  Standardization (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>