NIST Lightweight Cryptography Standardization

MELTEM SONMEZ TURAN

NIST

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

GLOBAL PLATFORM SECURITY TASK FORCE MEETING
MARCH 28, 2023

Overview of the Talk

1. NIST Computer Security Division – Overview

2. NIST Lightweight Cryptography Standardization Process

3. Evaluation of the Finalists and the Selection of Ascon

4. Next steps

National Institute of Standards and Technology

Non-regulatory federal agency within U.S. Department of Commerce.

Founded in 1901, known as National Bureau of Standards (NBS) prior to 1988.

3,400+
FEDERAL EMPLOYEES

3,500+
ASSOCIATES

5
NOBEL PRIZES

MISSION

to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Laboratory Programs → Information Technology Lab → Computer Security Division

Computer Security Division (CSD)

Developing Crypto Standards

- International "competitions" e.g., AES, SHA-3, PQC, Lightweight Crypto
- Adoption of existing standards e.g., RSA, HMAC
- Open call for proposals: e.g., block cipher modes of operations

CSD Publications

- Federal Information Processing Standards (FIPS): Specify approved crypto standards
- NIST Special Publications (SPs): Guidelines, technical specifications, recommendations etc.
- NIST Internal or Interagency Reports (IR): Reports of research findings

Principles

Transparency, openness, balance, integrity, technical merit, global acceptability, usability, continuous improvement, innovation and intellectual property etc.

Lightweight Cryptography – Motivation

NIST

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

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

Call for Submissions and Requirements

In August 2018, NIST published ‘*Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process*’. **Submission deadline**: February 2019

Requirements

Security requirements

At least 112-bit security level for messages up to 2^{50} bytes, etc.

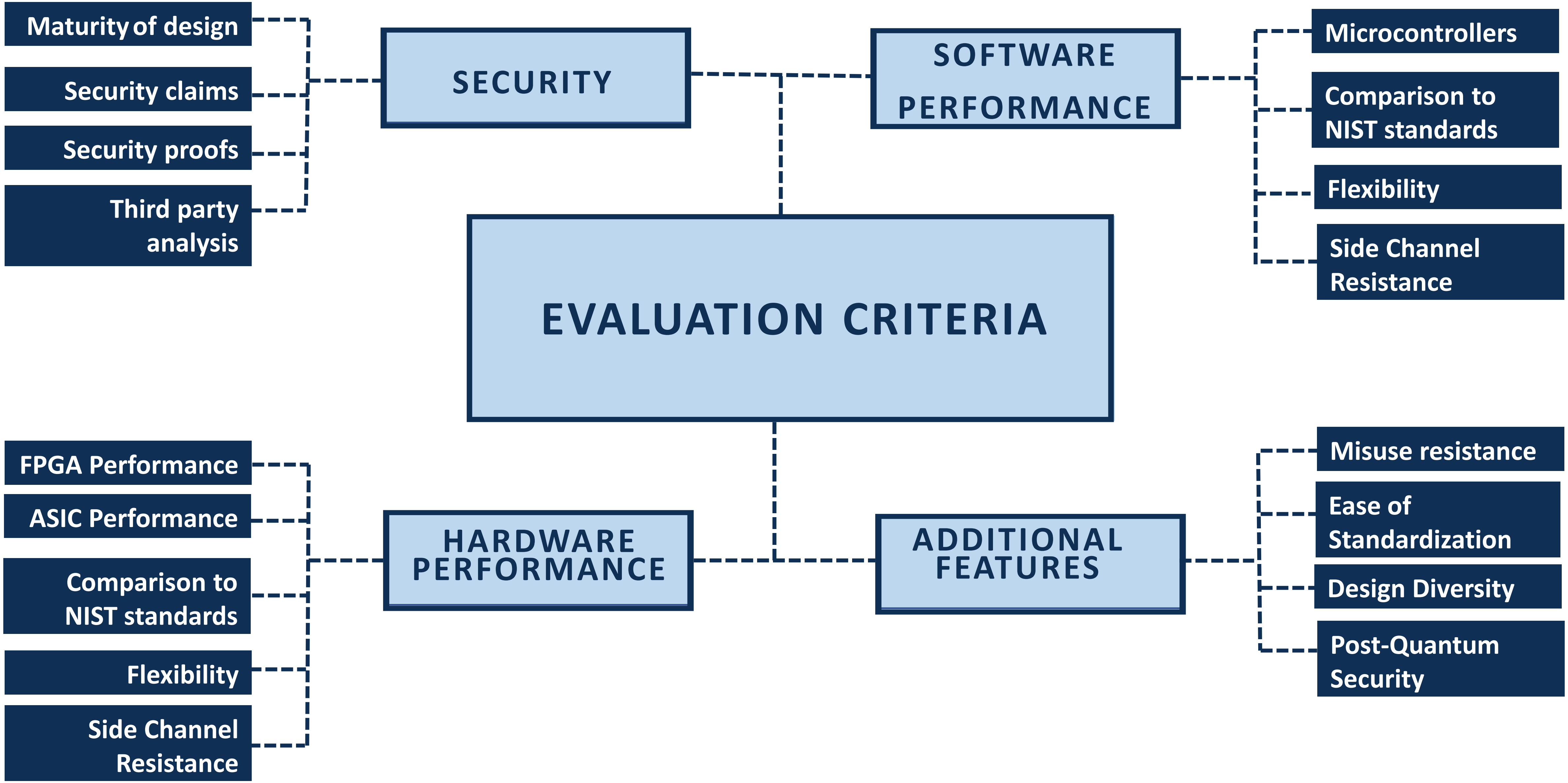
Design requirements

Perform better than NIST standards, optimized for short messages etc.

Implementation requirements

Reference and optimized implementation compatible with API etc.

Evaluation Criteria



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

Date	*Event*
July 2015	First Lightweight Cryptography Workshop at NIST
October 2016	Second Lightweight Cryptography Workshop at NIST
March 2017	Publication – NISTIR 8114 Report on Lightweight Cryptography
August 2018	Submission call
February 2019	Submission deadline
April 2019	Announcement of the first-round candidate
August 2019	Announcement of the second-round candidates
October 2019	NISTIR 8268, First Round Status Report
November 2019	Third Lightweight Cryptography Workshop at NIST
October 2020	Fourth Lightweight Cryptography Workshop (virtual)
March 2021	Announcement of the finalists
July 2021	NISTIR 8369, Second Round Status Report
May 2022	Fifth Lightweight Cryptography Workshop (virtual)
February 2023	Announcement of the selection
June 2023	Sixth Lightweight Cryptography Workshop (virtual)

Rounds of Evaluation

Round 1

April 2019 – August 2019

56 Round–1 Candidates

Evaluation based on security

Round 2

August 2019 – March 2021

32 Round–2 Candidates

Evaluation based on security and performance

Round 3

March 2021 – February 2023

10 Finalists

Evaluation based on security, performance (including protected implementations) and additional features

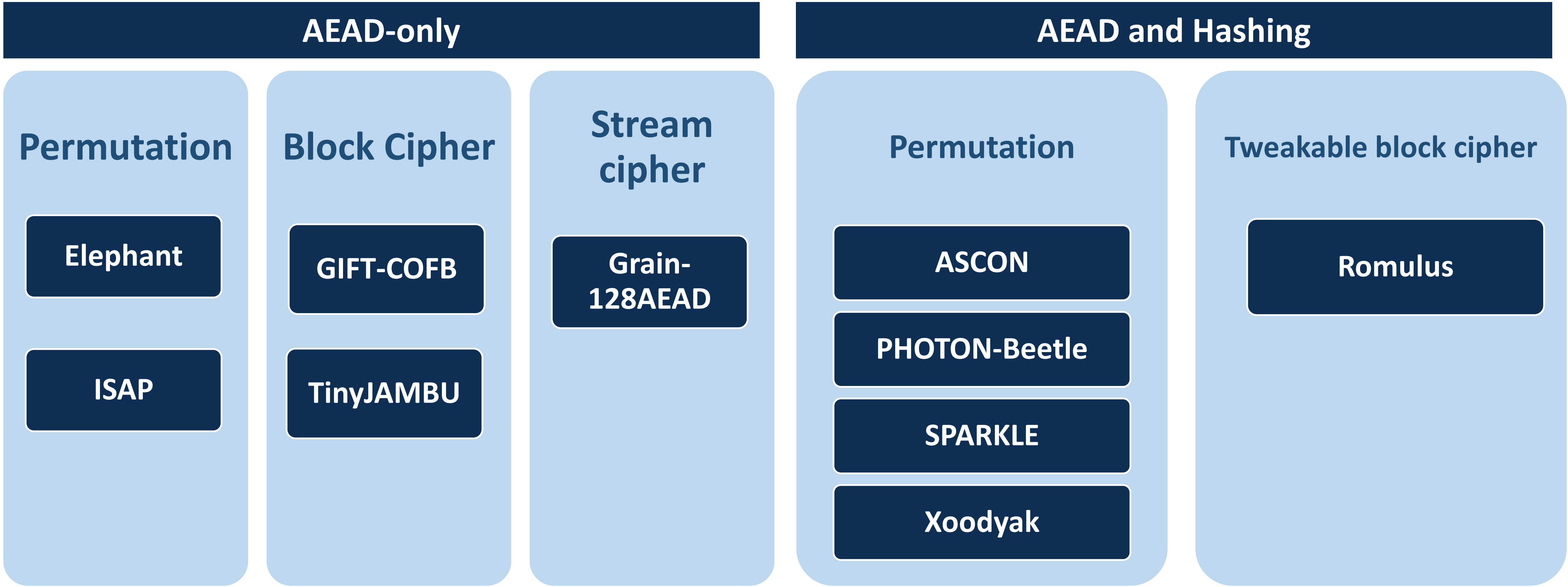
Finalists

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

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 of the Finalists



AEAD-only			AEAD and Hashing	
Permutation	Block Cipher	Stream cipher	Permutation	Tweakable block cipher
Elephant	GIFT-COFB	Grain-128AEAD	ASCON	Romulus
ISAP	TinyJAMBU		PHOTON-Beetle	
			SPARKLE	
			Xoodyak	

Software Benchmarking

Microcontroller benchmarking by NIST LWC Team

Devices:

- 8-bit AVR
- 32-bit ARM Cortex M0+, M4, M3
- 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:

- ROM, RAM usage
- Speed

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

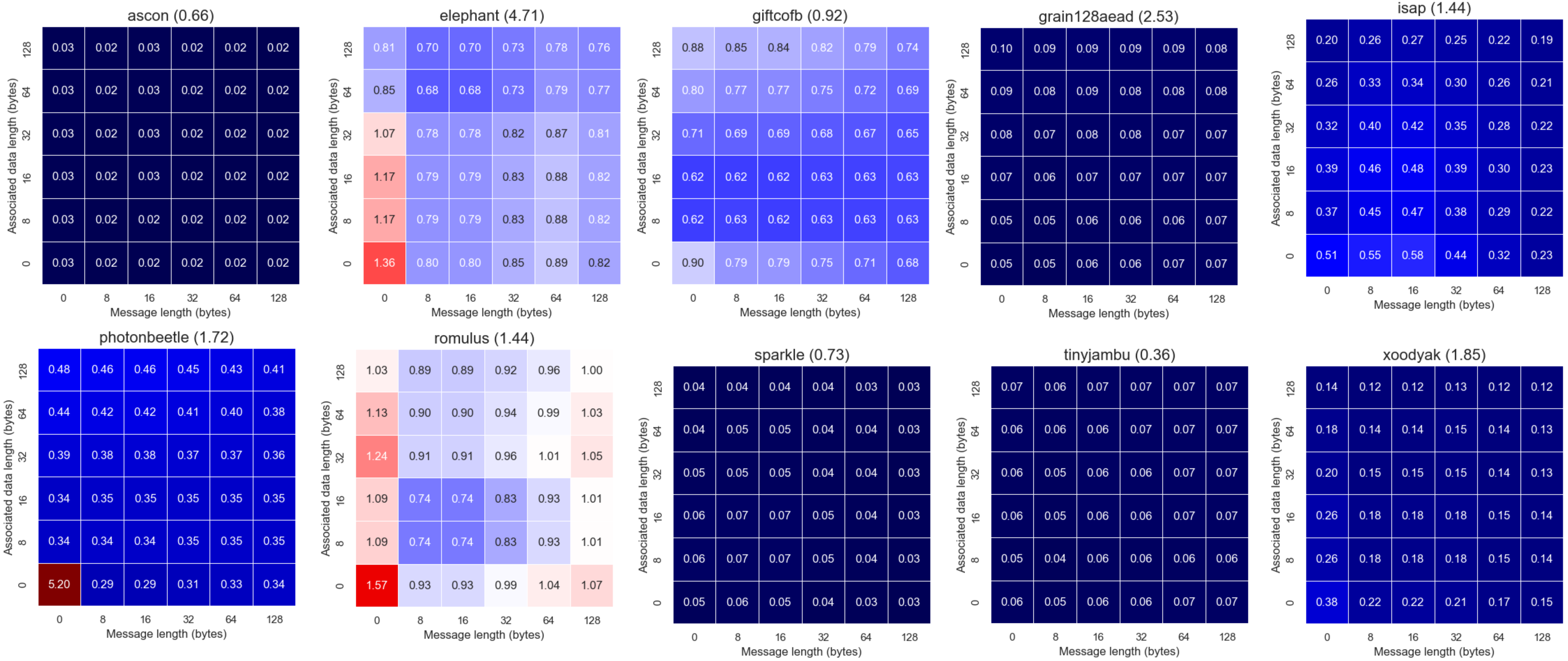
Metrics:

- Speed

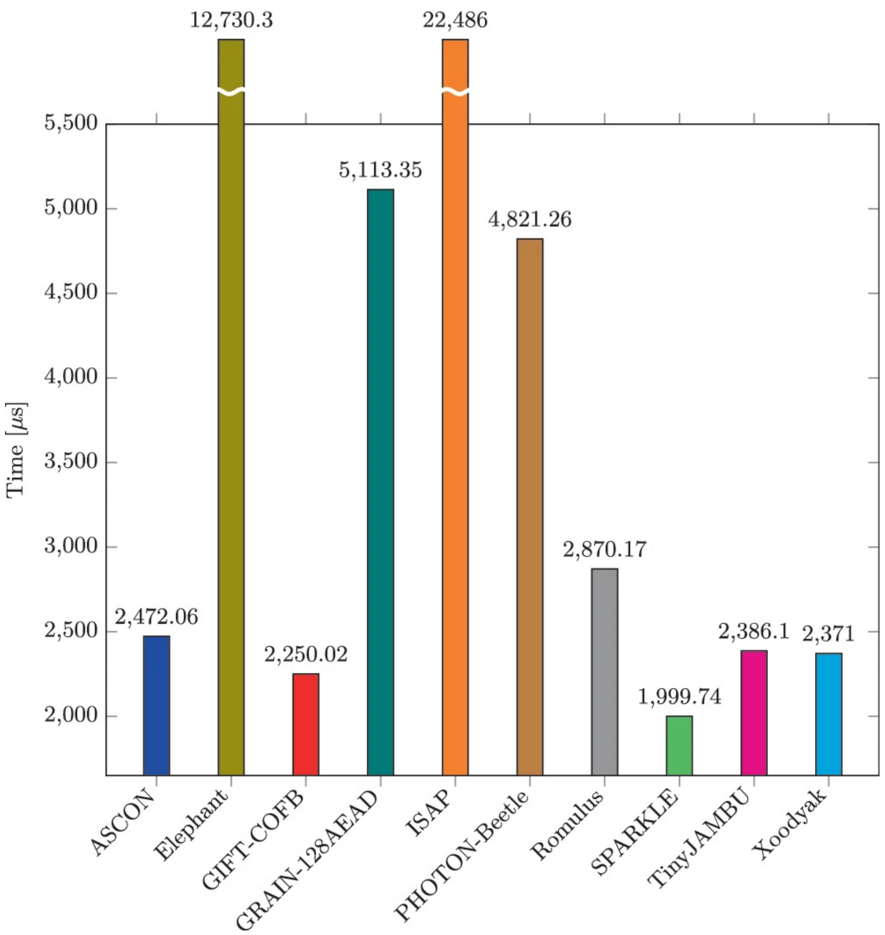
Number of available SW implementations

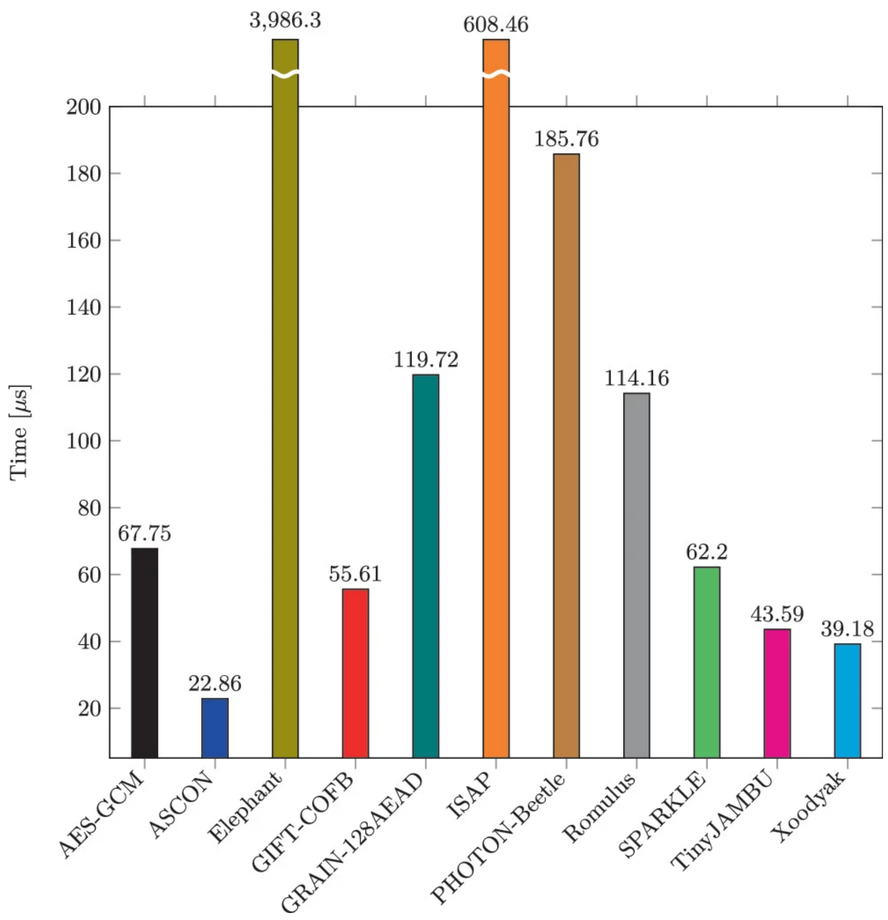
Finalist	#AEAD	#Hash	#Combined	Total
Ascon	120	110	52	282
Elephant	6	-	-	6
GIFT-COFB	11	-	-	11
Grain-128aead	6	-	-	6
ISAP	37	-	-	37
PHOTON-Beetle	20	10	16	46
Romulus	32	11	27	70
Sparkle	25	13	3	41
TinyJambu	9	-	-	9
Xoodyak	9	8	1	18
Total	**275**	**152**	**99**	**526**

Comparison with AES-GCM

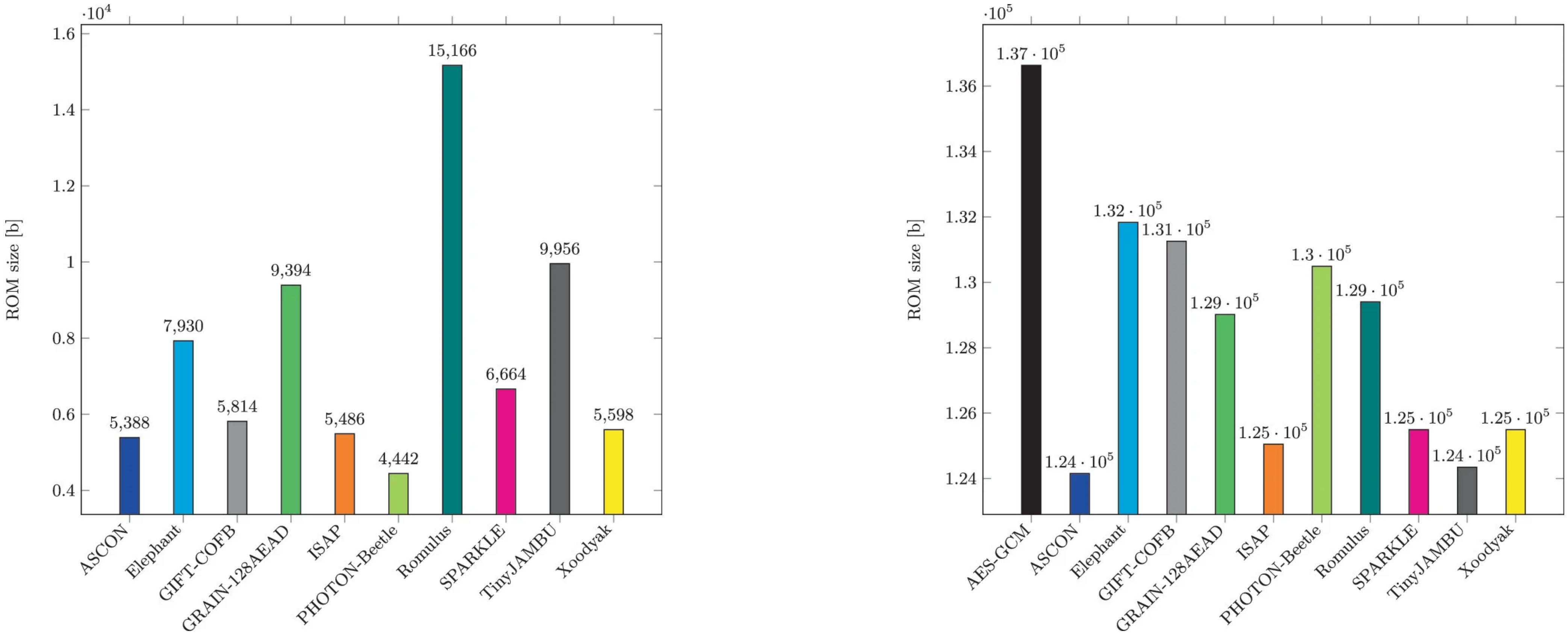


Execution time ratio of smallest primary AEAD implementations to AES-GCM on nRF52840



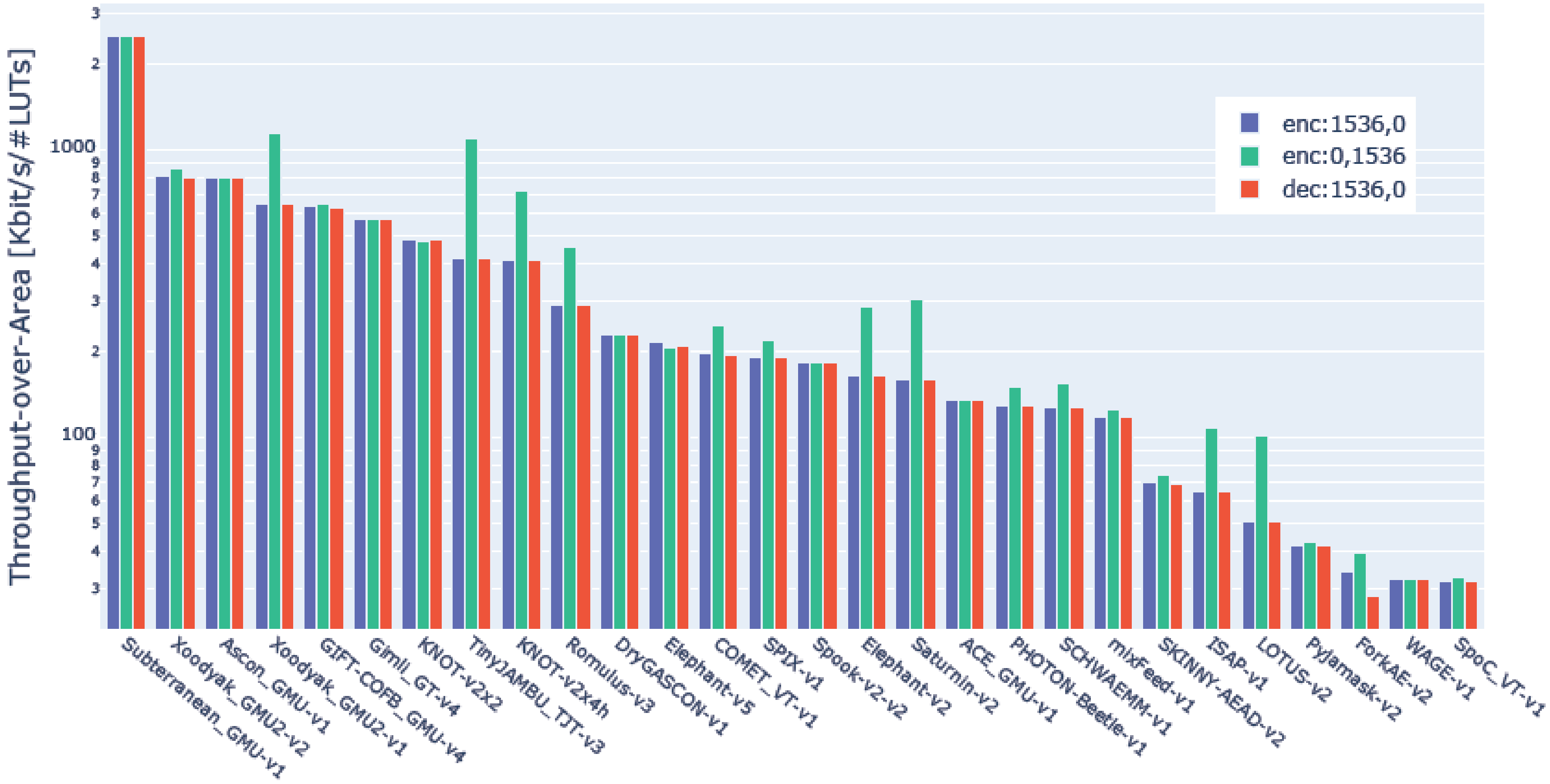


Speed comparison on Arduino Uno and ESP32 by Renner et al.



Code size comparison on Arduino Uno and Maixduino by Renner et al.

Hardware Benchmarking (Round 2)



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

The Selection Process

- Fair evaluation of finalists is challenging.
  - Assigning weights for different evaluation criteria (security, performance in software and hardware, design maturity, amount of third-party analysis, IP issues, etc.)
  - Different security claims, different functionality, attacks with different complexities etc.
  - Limited resources (not all algorithms got the same attention from the crypto community)
- Decision relied on publicly available analysis and benchmarking results.
- In February 2023, NIST announced the Ascon family as the winner.
  - Large amount of third-party analysis
  - AEAD variants were listed part of the CAESAR portfolio for ‘lightweight applications’.
  - No tweak
  - Performance advantage over NIST standards in software and hardware

Next Steps

- Publication of the third–round status update

- Sixth Lightweight Cryptography Workshop in June 21-22 2023 (virtual)

  Submission deadline: May 1, 2023

  Aim: to explain the selection process, and to discuss various aspects of lightweight cryptography standardization, such as

  - Which ASCON variants to standardize? All of subset ? XOF instead of hash?
  - Additionally functionality, e.g. dedicated MAC?
  - Support for additional parameter sizes? e.g., larger nonce, shorter tags

- Publication of draft standard (in 2023)

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