Final Steps of the NIST Lightweight Cryptography Standardization

MELTEM SONMEZ TURAN
NIST Lightweight Cryptography Team

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

METU IAM Colloquium
MAY 2, 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

- Part of US Department of Commerce
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988

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.

3,400+
FEDERAL EMPLOYEES

3,500+
ASSOCIATES

5
NOBEL PRIZES

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.

advanced encryption standard

1. Leech et al., *The Economic Impacts of the Advanced Encryption Standard*, 2018
2. Smid, Development of the Advanced Encryption Standard, 2021
3. Mouha, NISTIR 8319 Review of the Advanced Encryption Standard, 2021

Why do the crypto community continue designing new symmetric-key primitives?

New applications

Format preserving encryption, searchable encryption, order-preserving encryption, white-box cryptography, ciphers to be used in protocols (e.g., multi-party computation, zero-knowledge proofs), full-disk encryption, etc.

New features

Nonce-misuse resistance, combined functionality, inherent side channel resistance, related-key security, post-quantum security, key commitment, RUP security, *suitable for constrained environments* etc.

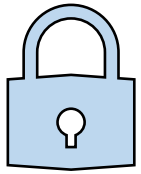
Lightweight Cryptography – Motivation

CONSTRAINED DEVICES

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

NEW APPLICATIONS

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



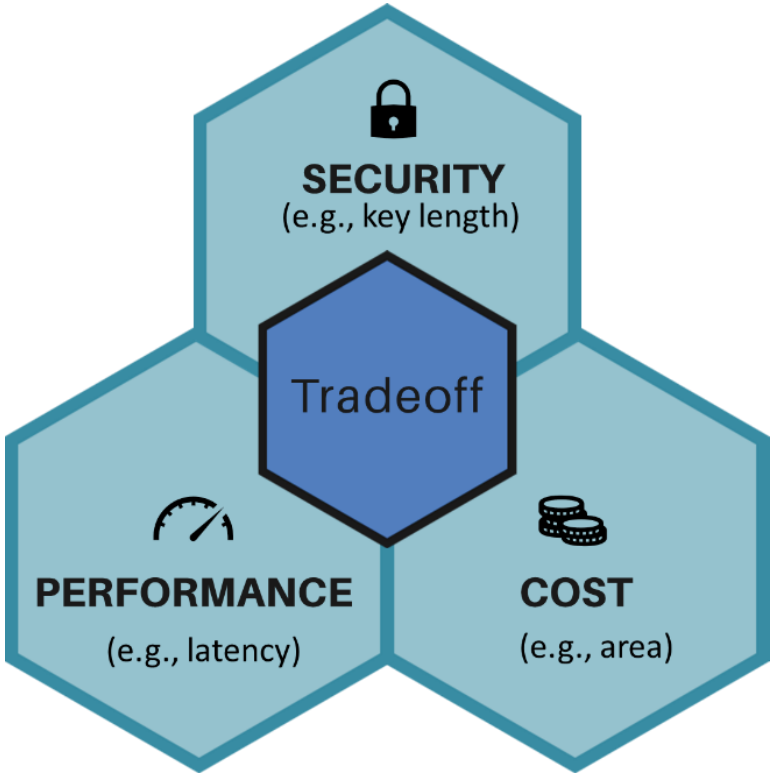
PRIVATE INFORMATION

e.g., location, health data

LACK OF CRYPTOGRAPHY STANDARDS

NIST crypto standards are optimized for general-purpose computers

Designing Lightweight Primitives



- Earlier designs
  - Shorter keys, smaller block sizes, smaller security margins by design.
- Newer designs
  - Many iterations of simple rounds, simple operations (e.g., 4x4 Sboxes, bit permutations), simpler key schedules
- Engineering challenge

Weight of an Algorithm

Weight of an algorithm is a property of its implementation depending on different metrics of the target platform.

Hardware applications

Area, latency, power consumption, throughput etc.

Software applications

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

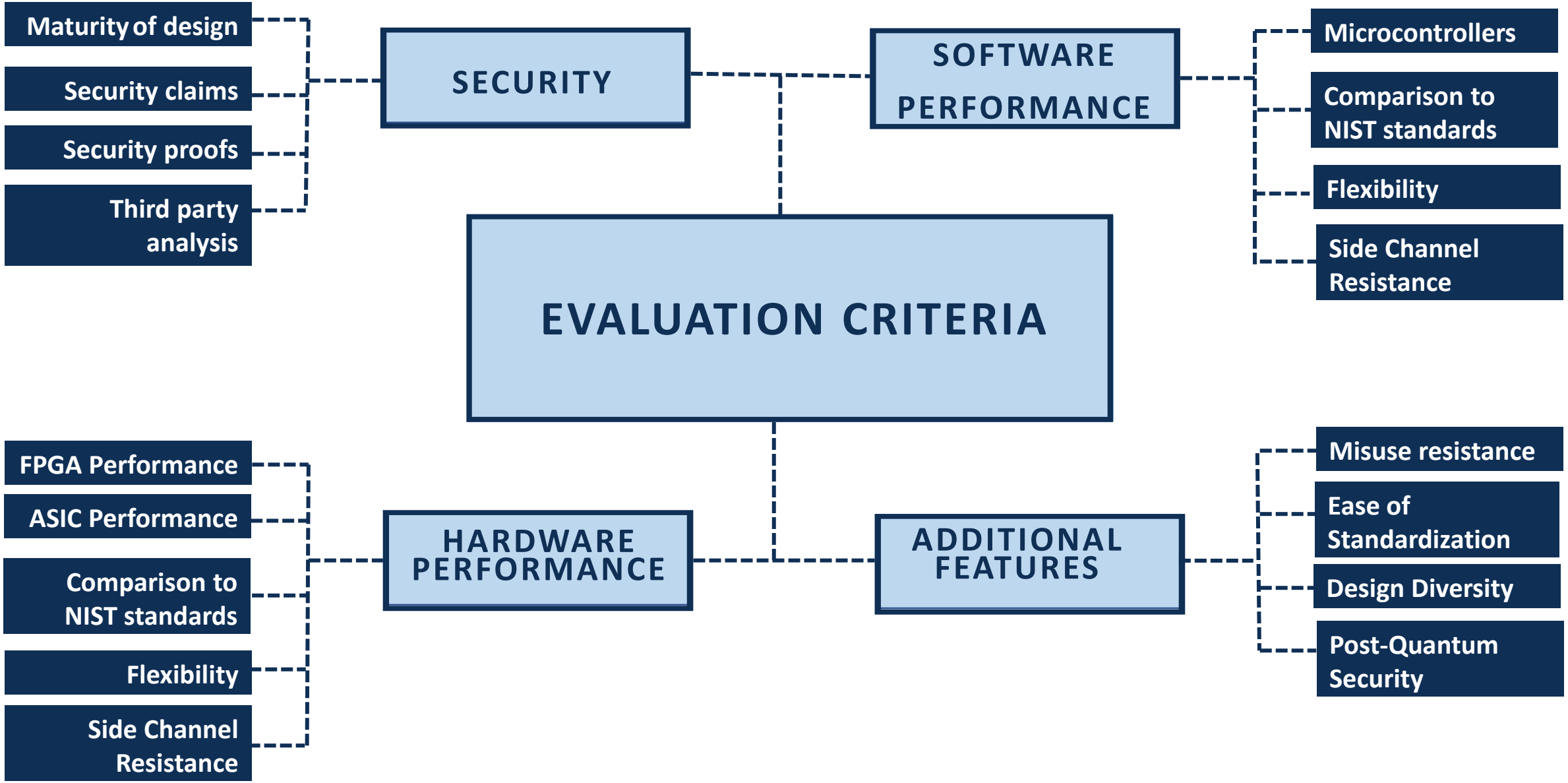
Requirements

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



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)

Evaluation through Rounds

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 and performance (including protected implementations)

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

NIST

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

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:
- 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

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	1	4	42
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**	**153**	**103**	**531**

Benchmarking by NIST

Code size

Flash use of compiled executable for AEAD or hashing, as reported by PlatformIO.

For AEAD, compiled with support for:

- Authenticated encryption only
- Decryption-verification only
- Both encryption and decryption

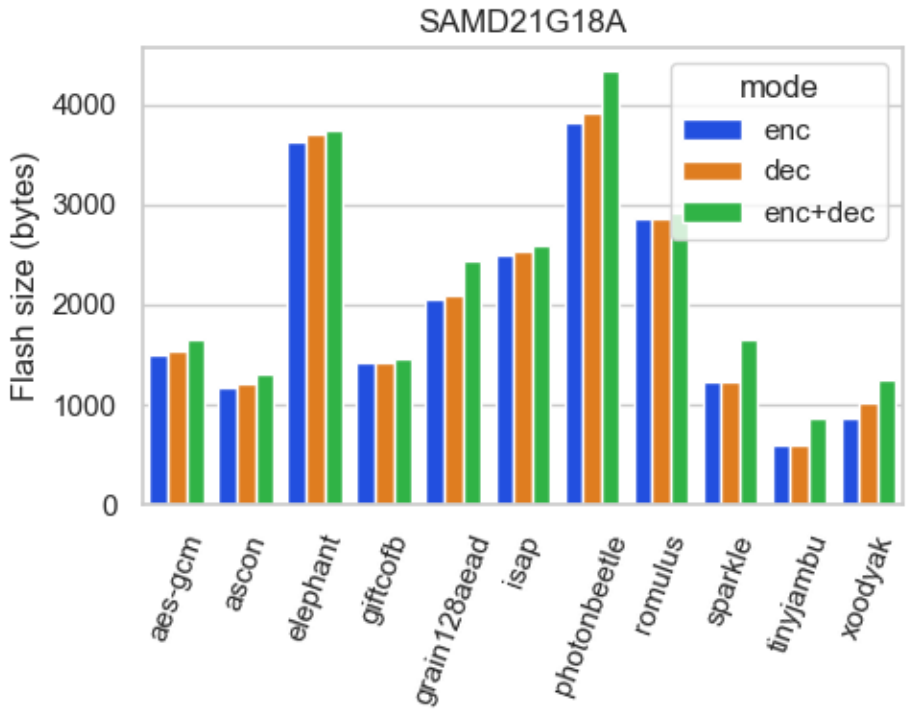
Execution time

Ratio of candidate execution time over AES-GCM execution time for AEAD and hashing with various input lengths.

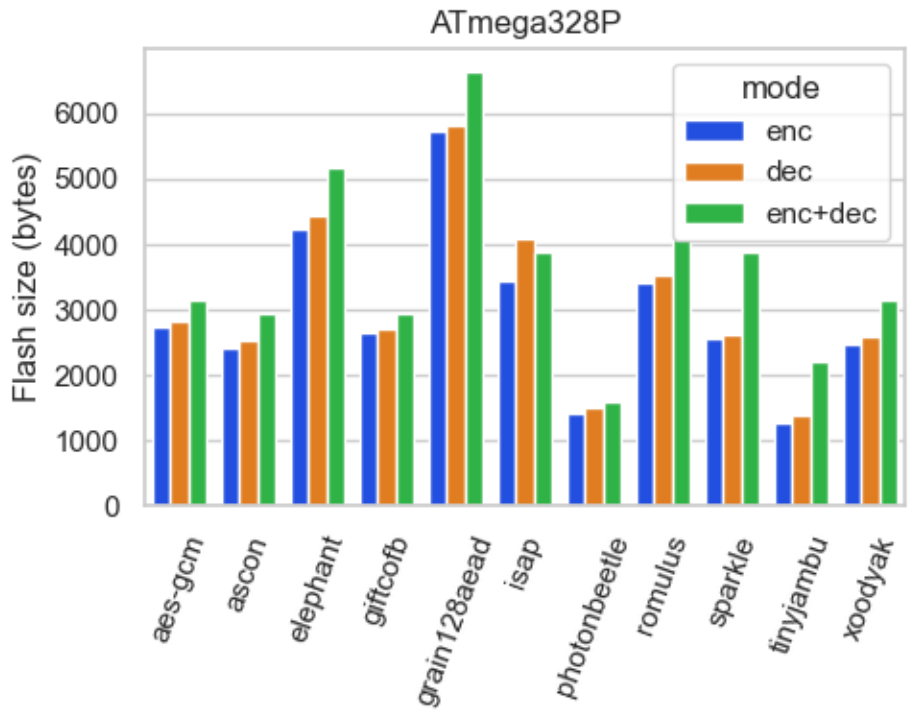
Combined size

The code size of combined implementations (when available).

Smallest AEAD

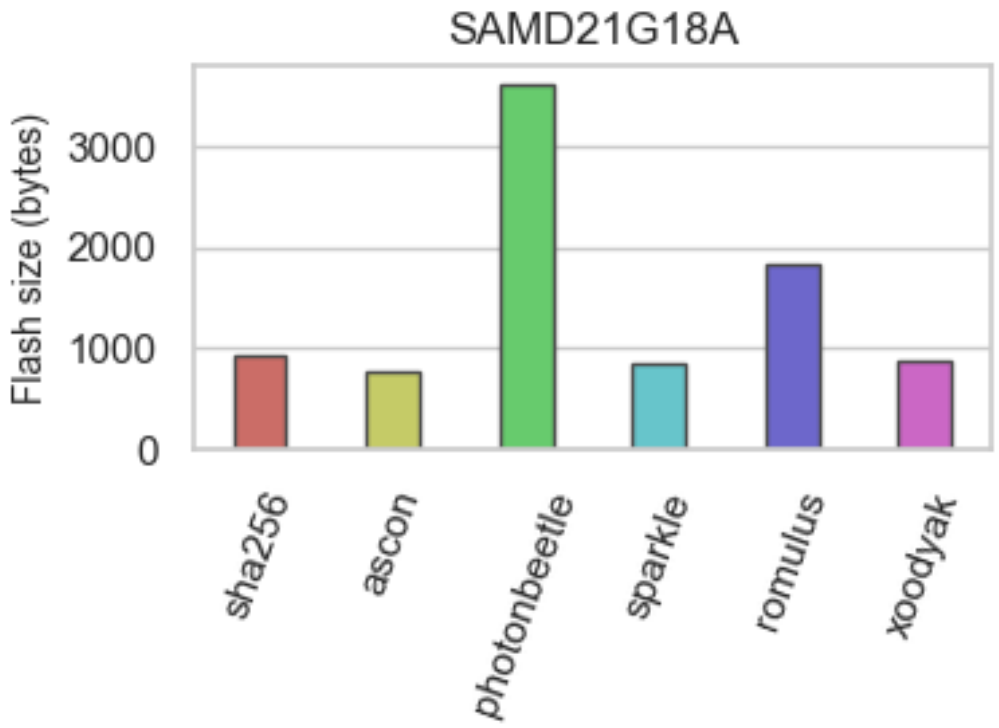


32-bit ARM Cortex-M0+

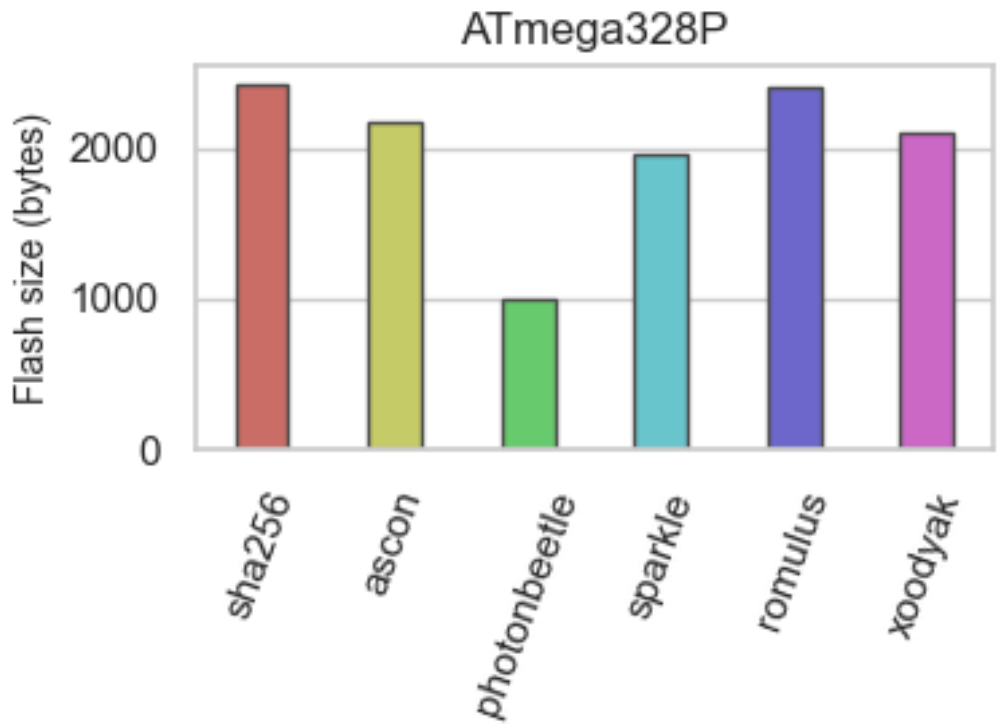


8-bit AVR

Smallest hashing

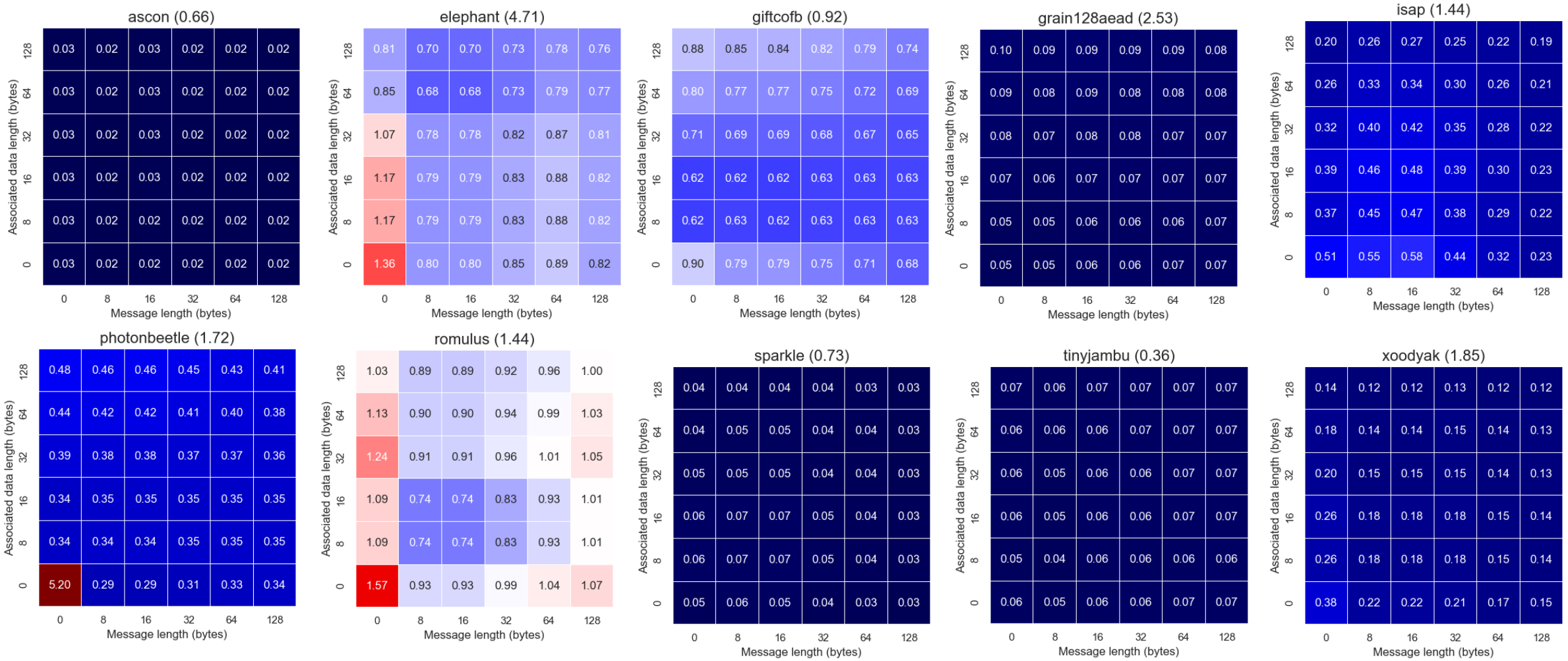


32-bit ARM Cortex-M0+



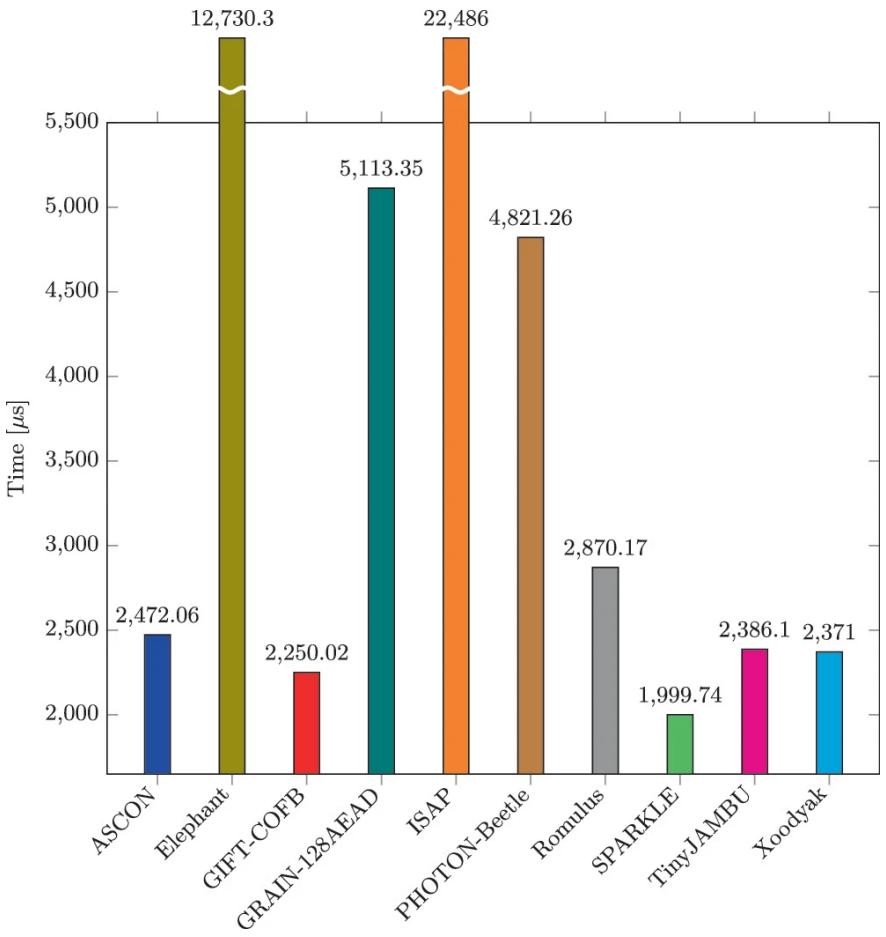
8-bit AVR

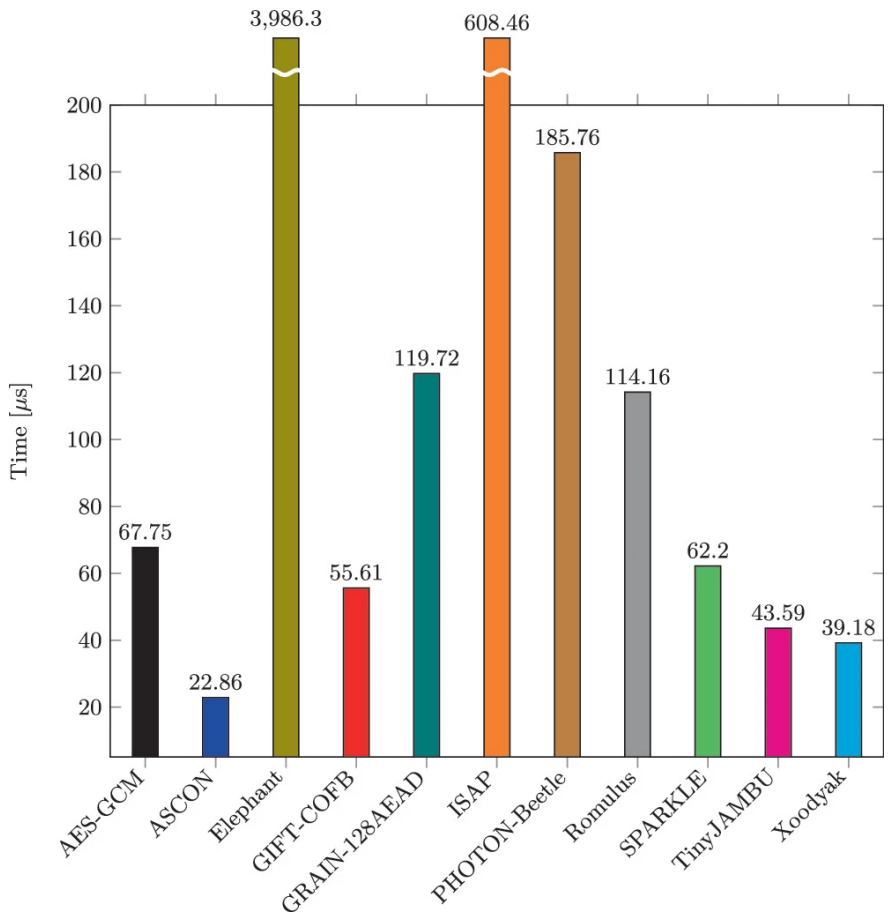
Execution time



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

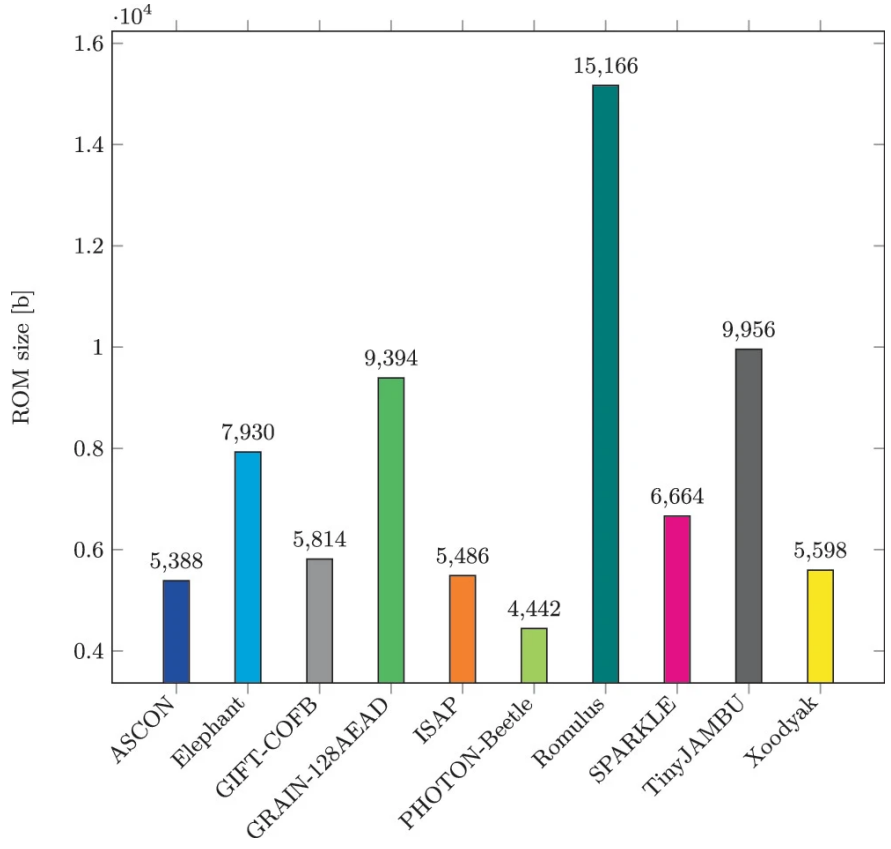
Benchmarking by Renner et al.

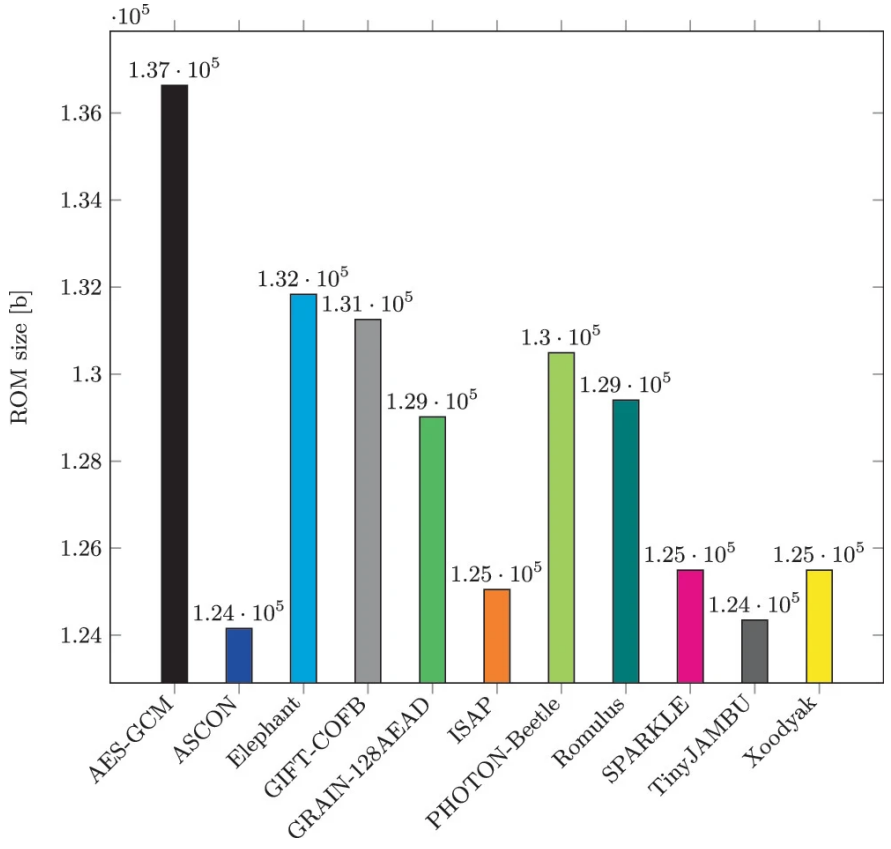




Speed comparison on Arduino Uno and ESP32 by Renner et al.

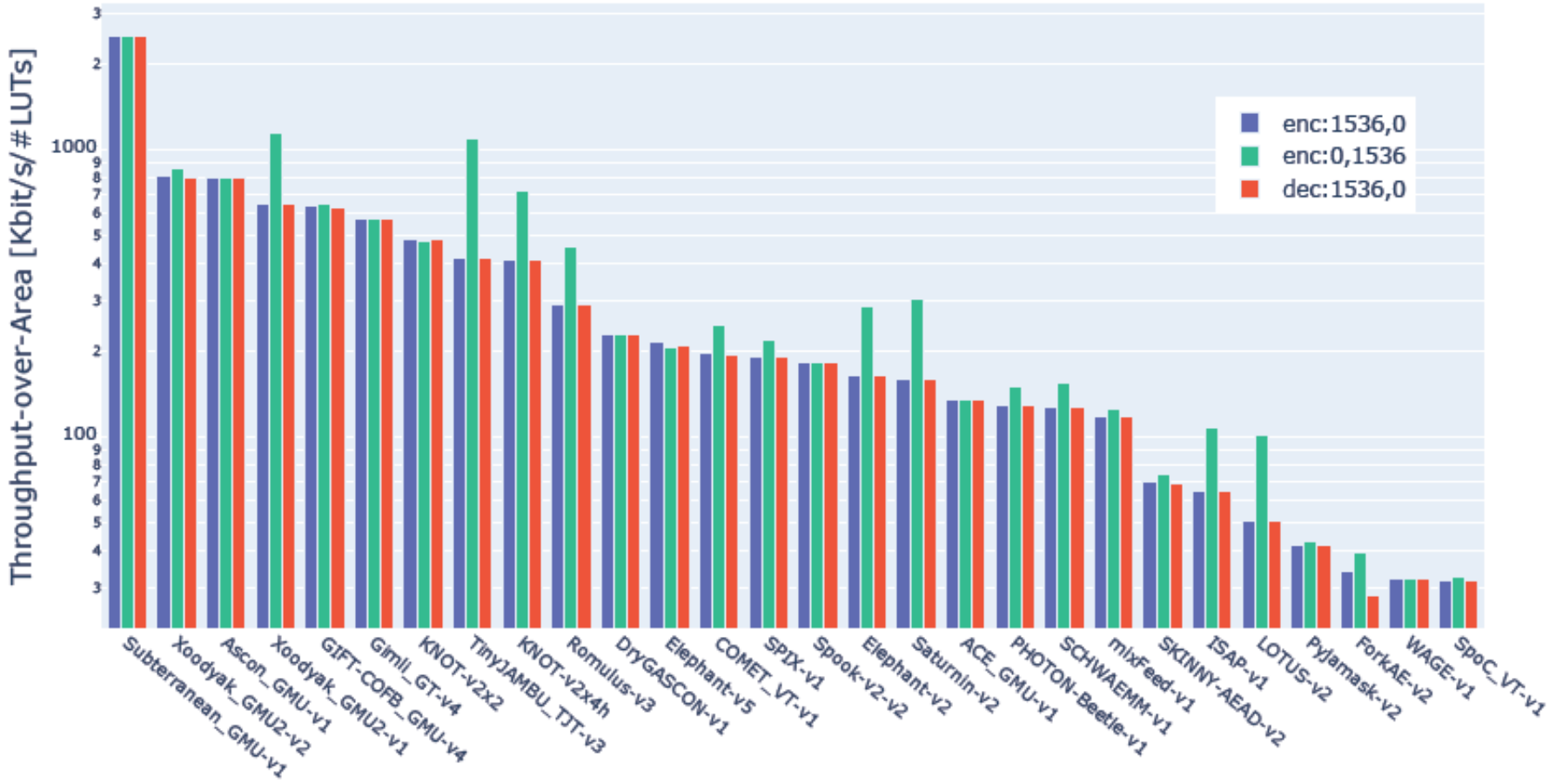
Benchmarking by Renner et al.





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

Round 2 Hardware Benchmarking



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 different weights for different 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 Ascon family as the winner.
  - Large amount of third-party analysis
  - AEAD variants were listed part of the CAESAR portfolio for constrained devices.
  - 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 AEAD 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)

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