Heavyweight Protection via *Lightweight Cryptography*

Meltem Sönmez Turan

NIST Lightweight Cryptography Team

Real World Cryptography 2022 – April 13, 2022

advanced encryption standard

1. Smid, Development of the Advanced Encryption Standard, 2021
2. Leech et al., *The Economic Impacts of the Advanced Encryption Standard*, 2018
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, full-disk encryption, ciphers suitable for protocols like multi-party computation, zero-knowledge proofs, etc.

New features

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

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

LACK OF CRYPTOGRAPHY STANDARDS

NIST crypto standards are optimized for general-purpose computers

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

Code size, latency, throughput, RAM/ROM etc.

Anti-counterfeiting

- Most RAIN RFID chips have small amount of user memory (typically < 64 bits, some special chips have <2k bits).
- Hardware-oriented primitives with small area

Healthcare

- Measuring blood pressure, blood sugar, pulse etc.
- Hardware-oriented primitives by small energy requirements

Vehicle communication

- In-vehicle, vehicle-to-vehicle and road-to-vehicle communication, driving assistance systems
- Low latency, high throughput

Smart Home

- Electrical home appliances with low-end CPUs
- Software-oriented primitives that consume less CPU time and smaller ROM requirements

Designing Lightweight Primitives

- Engineering challenge
  - "Too much crypto"
- Earlier designs
  - Shorter keys, smaller block sizes, smaller security margins by design.
- Newer designs
  - Many iterations of simple rounds, simple operations (e.g., 4-bit s-boxes, bit permutations), simpler key schedules (e.g., sponge construction)

1. Jean-Philippe Aumasson, *Too Much Crypto*, RWC 2020

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

Security requirements

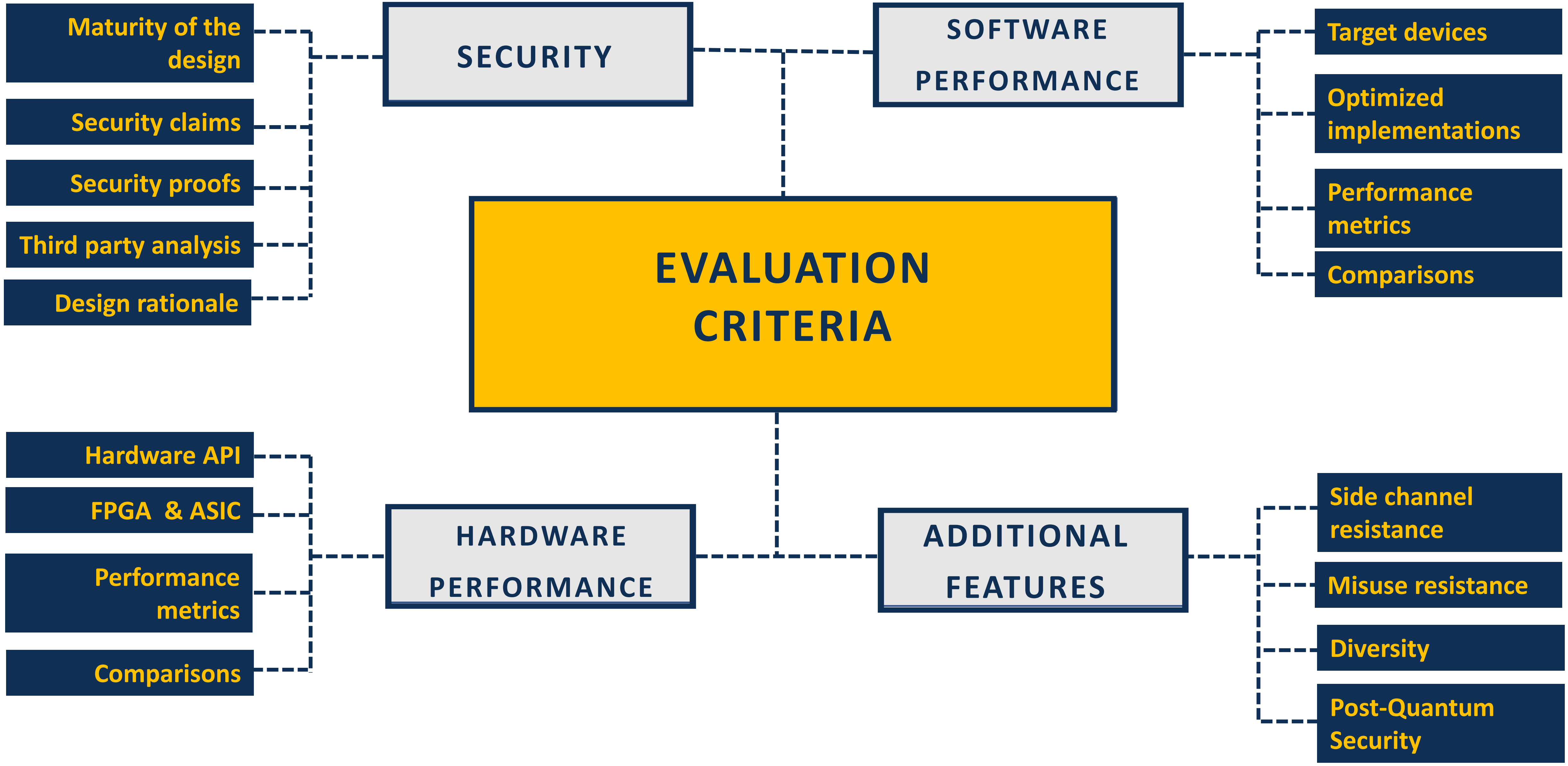
- Confidentiality + integrity
- At least 128-bit keys
- Plaintext up to 2^{50} bytes
- etc.

Design requirements

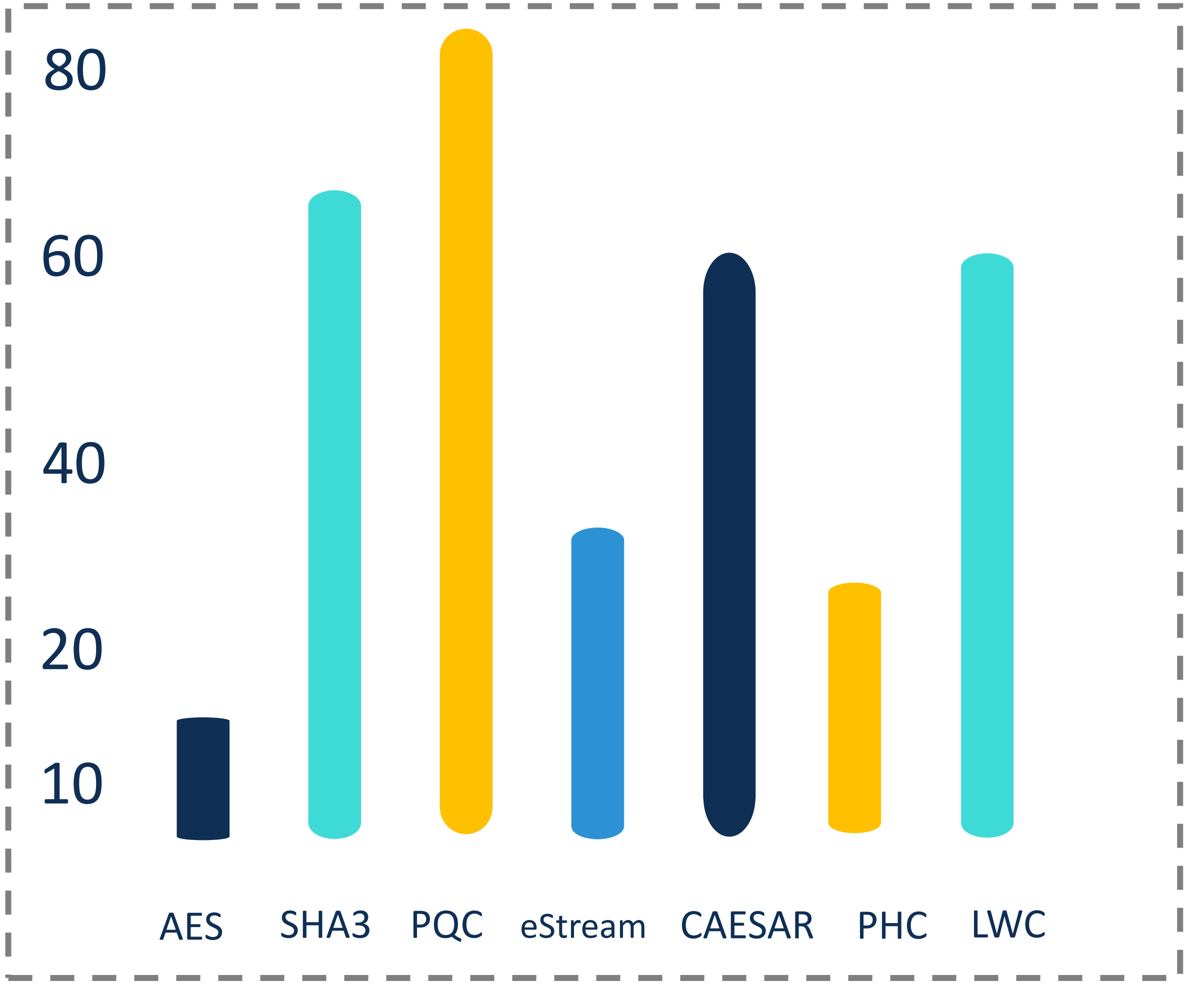
- Perform better than NIST standards
- Optimized for short messages
- etc.

Implementation requirements

- Reference and optimized implementation compatible with API
- etc.


EVALUATION CRITERIA
SECURITY
Maturity of the design
Security claims
Security proofs
Third party analysis
Design rationale
SOFTWARE PERFORMANCE
Target devices
Optimized implementations
Performance metrics
Comparisons
HARDWARE PERFORMANCE
Hardware API
FPGA & ASIC
Performance metrics
Comparisons
ADDITIONAL FEATURES
Side channel resistance
Misuse resistance
Diversity
Post-Quantum Security

SUBMISSIONS



NUMBER OF SUBMISSIONS

FROM 25 COUNTRIES

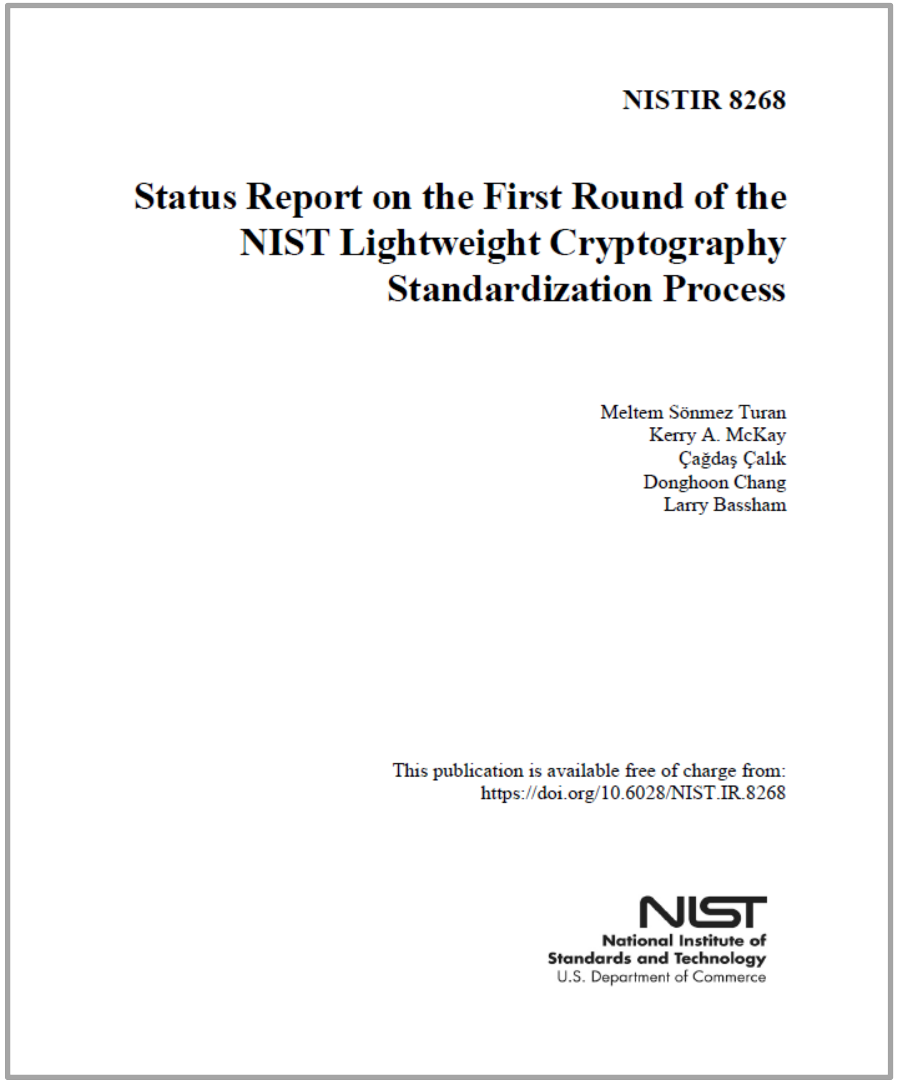
Round 1

Around 4 months

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

Candidates providing AEAD-only functionality

Permutation	Elephant, ISAP, Oribatida, SPIX, SpoC, Spook[3], WAGE
Block Cipher	COMET, GIFT-COFB, HyENA, mixFeed, Pyjamask, SAEAES, SUNDAE-GIFT, TinyJAMBU[1]
Tweakable Block Cipher	ESTATE, ForkAE, LOTUS-AEAD and LOCUS-AEAD, Romulus, Spook
Stream Cipher	Grain-128AEAD

Candidates providing AEAD and hashing functionalities

Permutation	ACE, ASCON, DryGASCON, Gimli, KNOT, ORANGE, PHOTON-Beetle, SPARKLE, Subterranean 2.0, Xoodyak
Block Cipher	SATURNIN[2]
Tweakable Block Cipher	SKINNY-AEAD and SKINNY-HASH

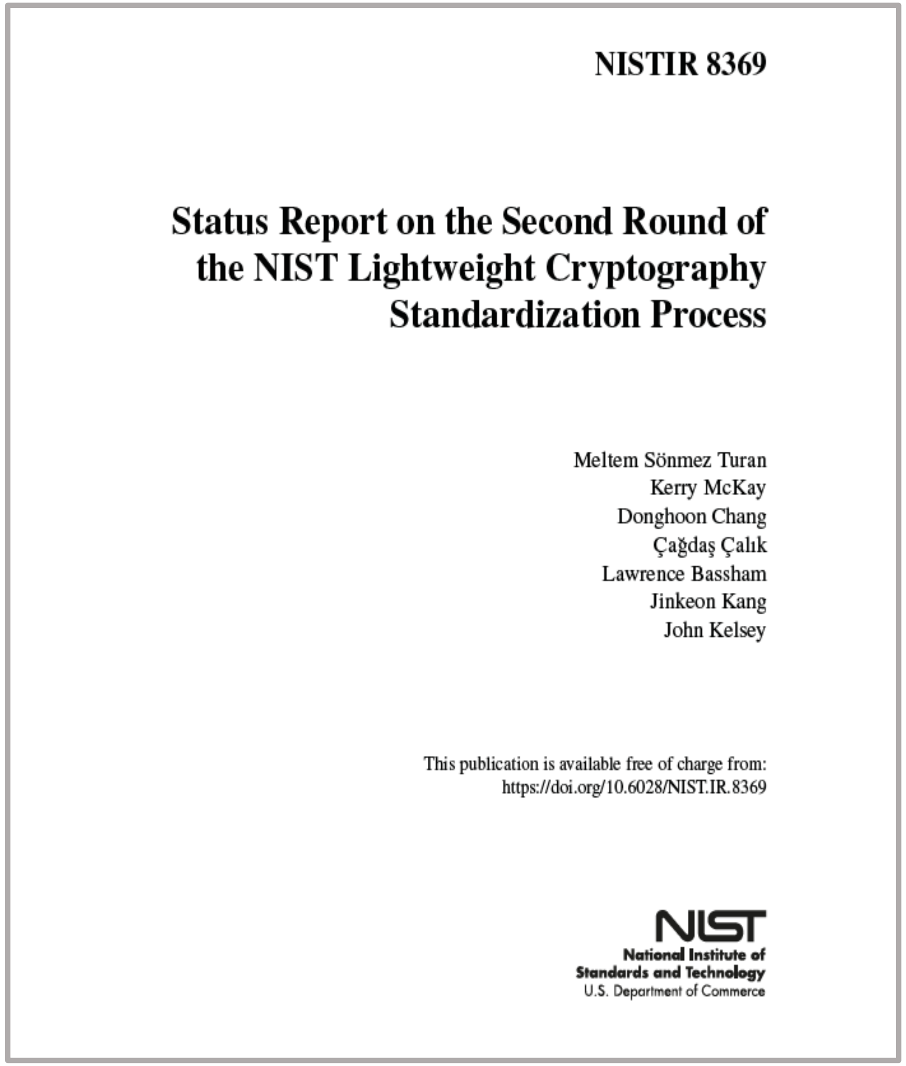
Round 2

Around 20 months (from Aug. 2019 to March 2021)

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

August 2020, status updates (optional)

Evaluation of the candidates were done based on their security and performance.



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

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

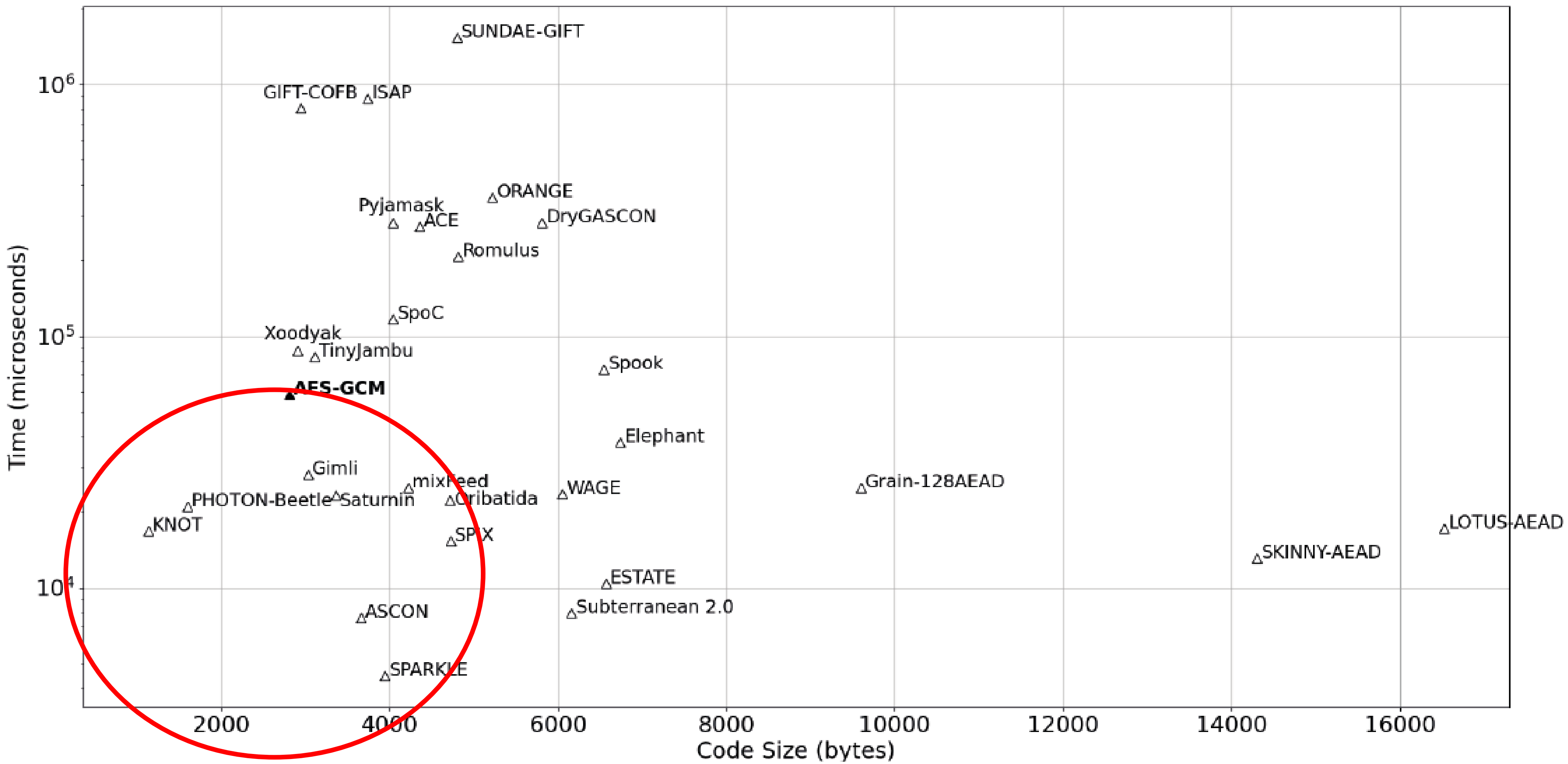
eBACS (ECRYPT Benchmarking of Cryptographic Systems) by Lange and Bernstein

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

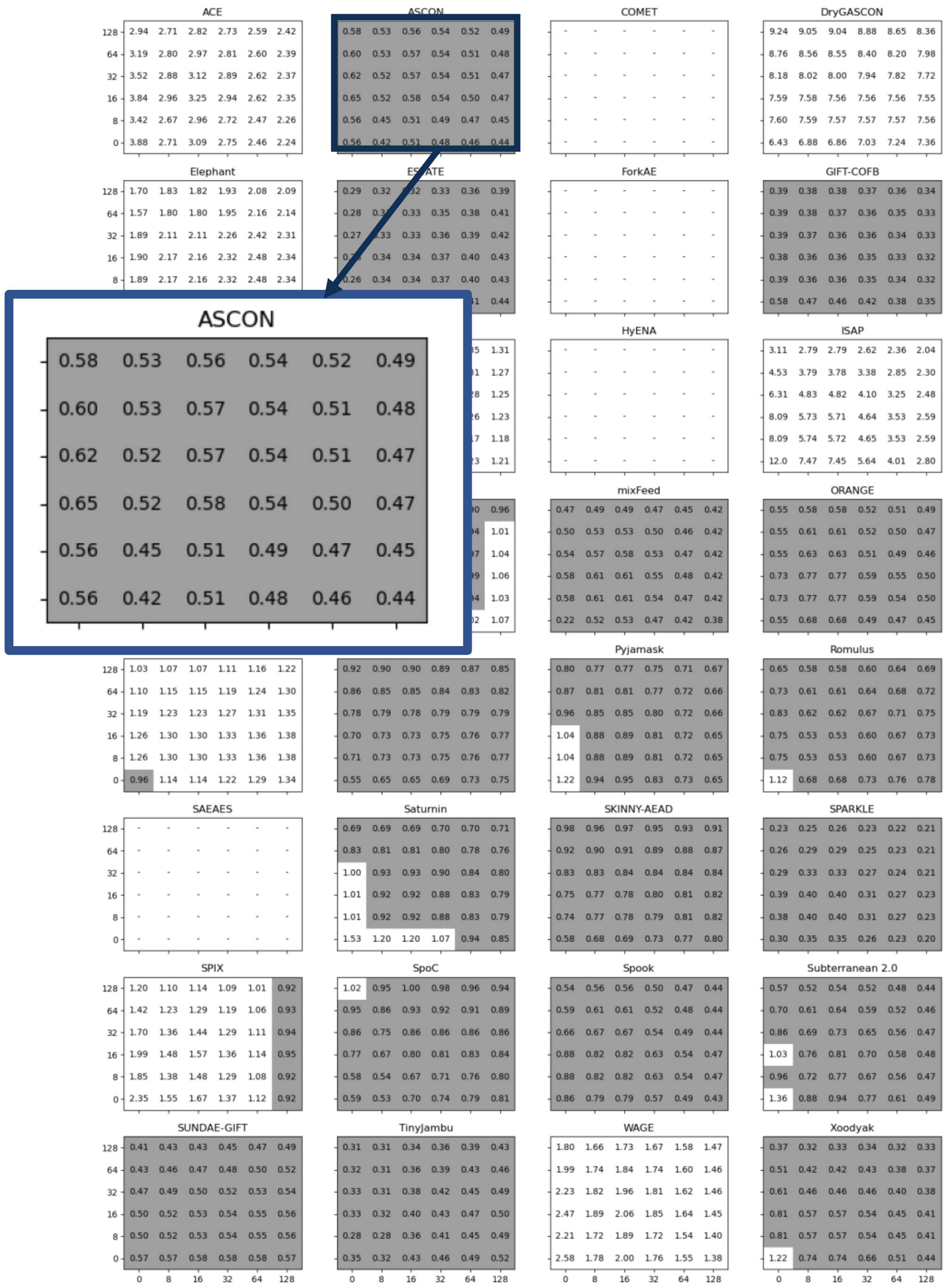
Relative timings for each candidate are shown by a matrix of values, where

- 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:

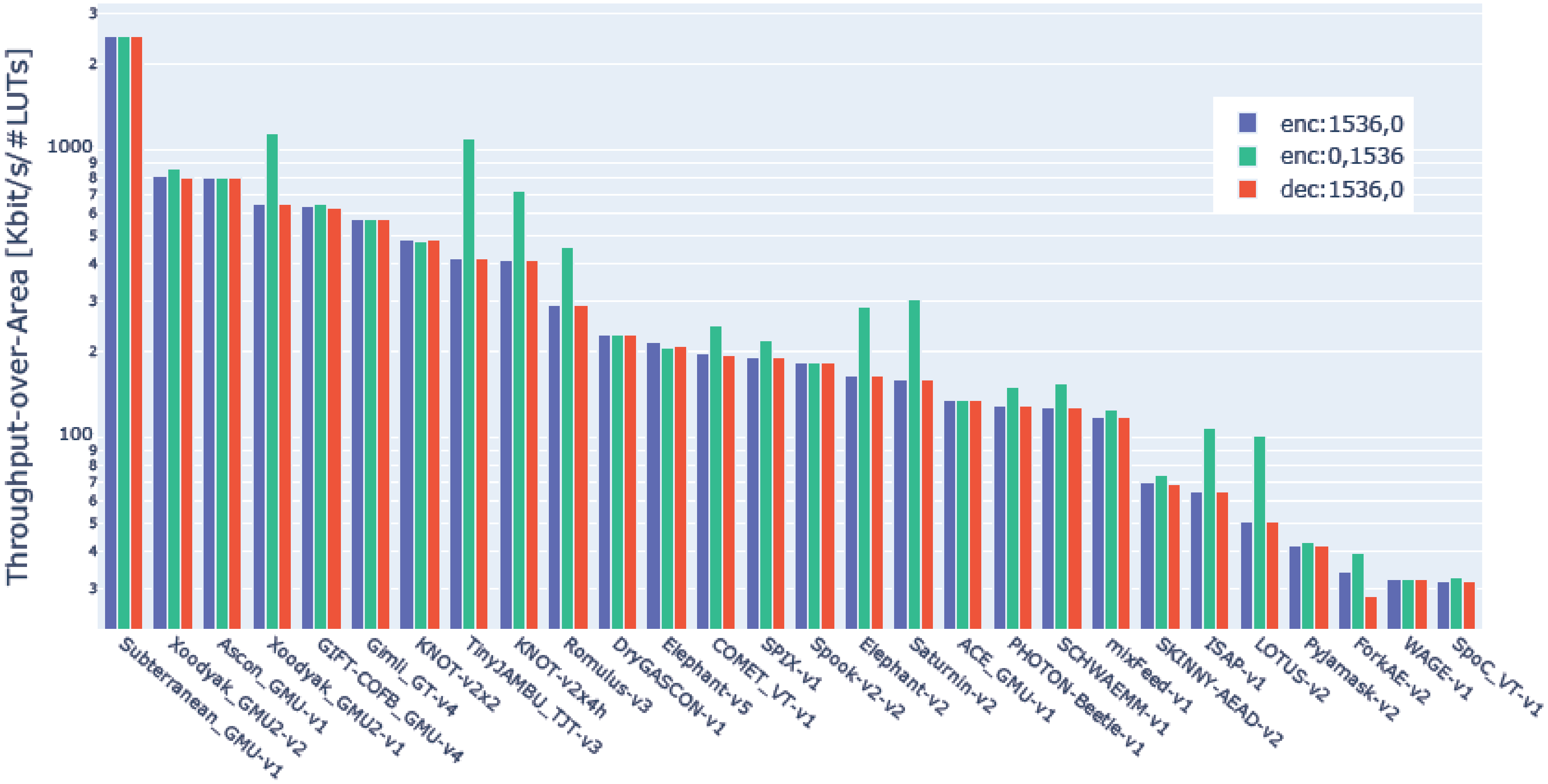
Ascon, Estate, Gimli, Knot, Lotus-AEAD, mixFeed, Orange, Photon-Beetle, Pyjamask, Romulus, Saturnin, Skinny-AEAD, Sparkle, Spoc, Spook, Subterranean, SUNDAE-GIFT, TinyJambu, Xoodyak perform better than AES-GCM on ATmega328P.



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)

Hardware Benchmarking



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

ACE	Gimli	Oribatida	SPIX
ASCON	Grain-128aead	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&Hash	Wage
GIFT-COFB	ORANGE	Sparkle	Xoodyak

Round 3

Ongoing (March 2021 --)

Finalists had the opportunity to update submission packages and propose tweaks to submissions.

Evaluation also includes side channel resistance.

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

Resistance to side-channel attacks

CERG from *George Mason University* proposes a general framework for evaluating side-channel resistance of LWC candidates using resources, experience, and general practices of the cryptographic engineering community developed over the last two decades.

Three calls

- for Side-Channel Security Validation Labs
- for Protected Hardware Implementations, targeting low-cost modern FPGAs
- for Protected Software Implementations, targeting low-cost modern embedded processors.


#NISTLWC
Lightweight Cryptography Workshop 2022
May 9-11, 2022 (Virtual Event)

2015-2018

First workshop
Second workshop
NISTIR 8114

2019

Submissions due
Round 1
NISTIR 8268
Round 2
Third workshop

2020 - 2021

Fourth workshop
Round 3
NISTIR 8369

2022

Fifth workshop

Next steps

- Evaluation of the finalists
- Fifth Lightweight Cryptography Workshop
- Selection of the winner(s) and status report publication
- Standardization

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