NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan and Kerry McKay
NIST Lightweight Cryptography Team

International Cryptographic Module Conference 2021
September 2, 2021

National Institute of Standards and Technology
U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

Outline

Background and Motivation

NIST Lightweight Cryptography Standardization

Next Steps

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

Application examples

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

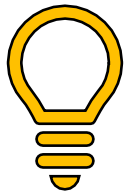
- Measuring blood pressure, blood sugar, pulse etc.
- Hardware-oriented primitives by small energy requirements

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

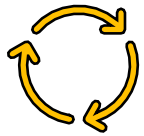


RESEARCH DEVELOPMENTS

e.g., permutation-based designs, simpler key schedules, inherent side channel resistance

GOAL

Develop new guidelines, recommendations and standards optimized for constrained devices



PROCESS

Public competition-like process with multiple rounds like AES, SHA3 and PQC standardization.

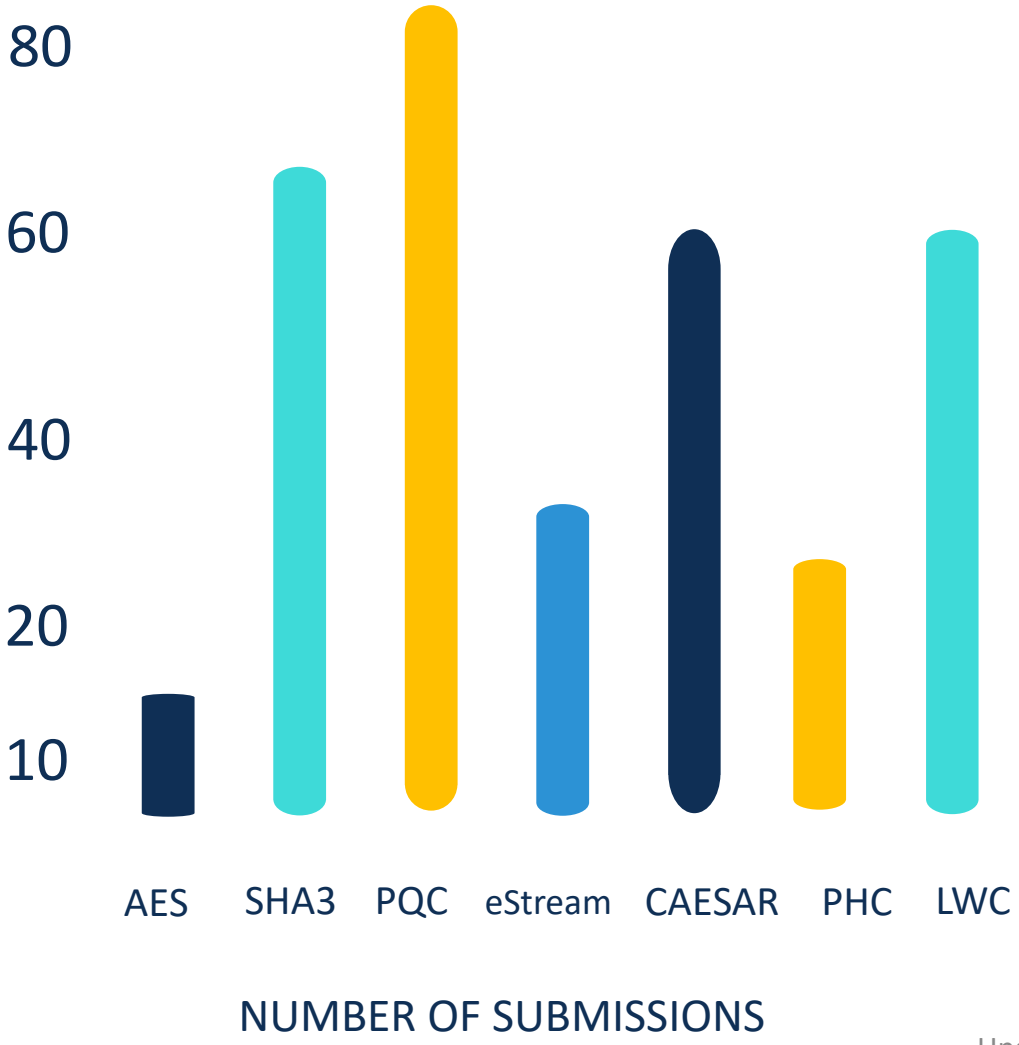
SCOPE

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

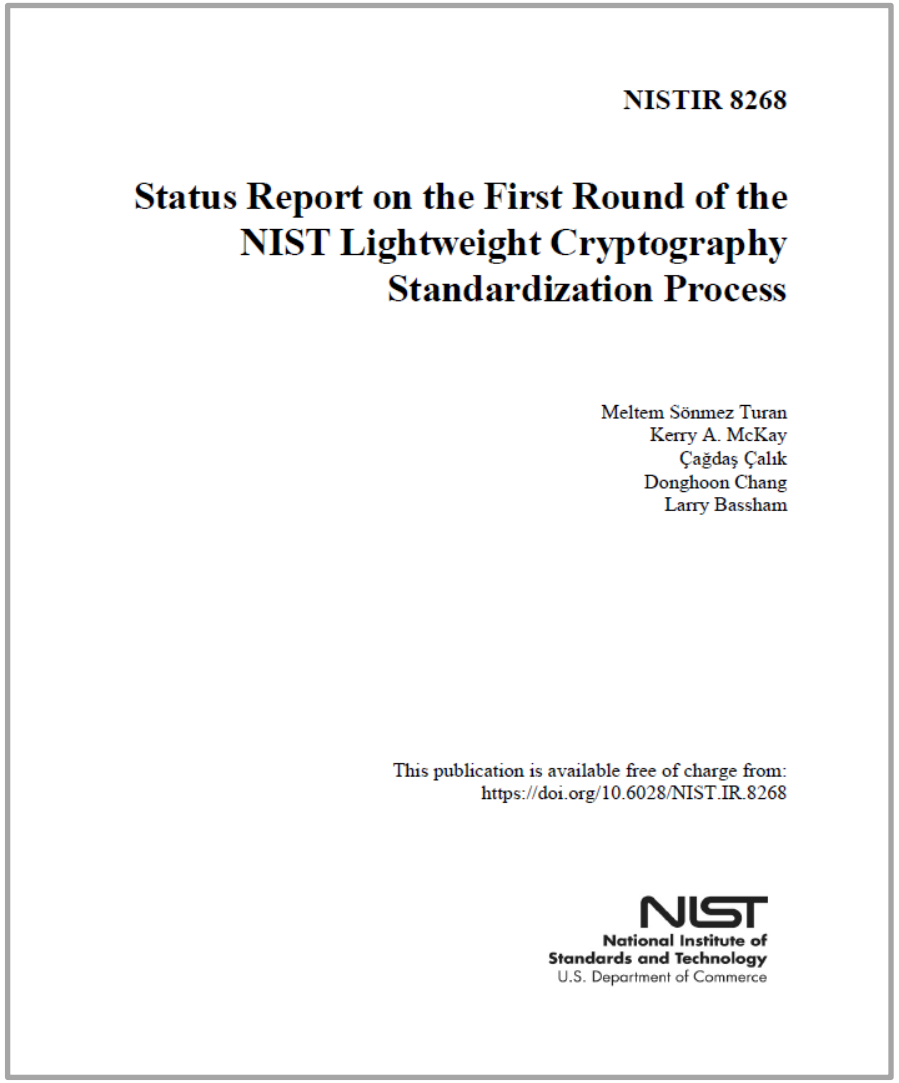
56 Round 1 Candidates



FROM 25 COUNTRIES

First Round of the Standardization Process

- 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*



NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

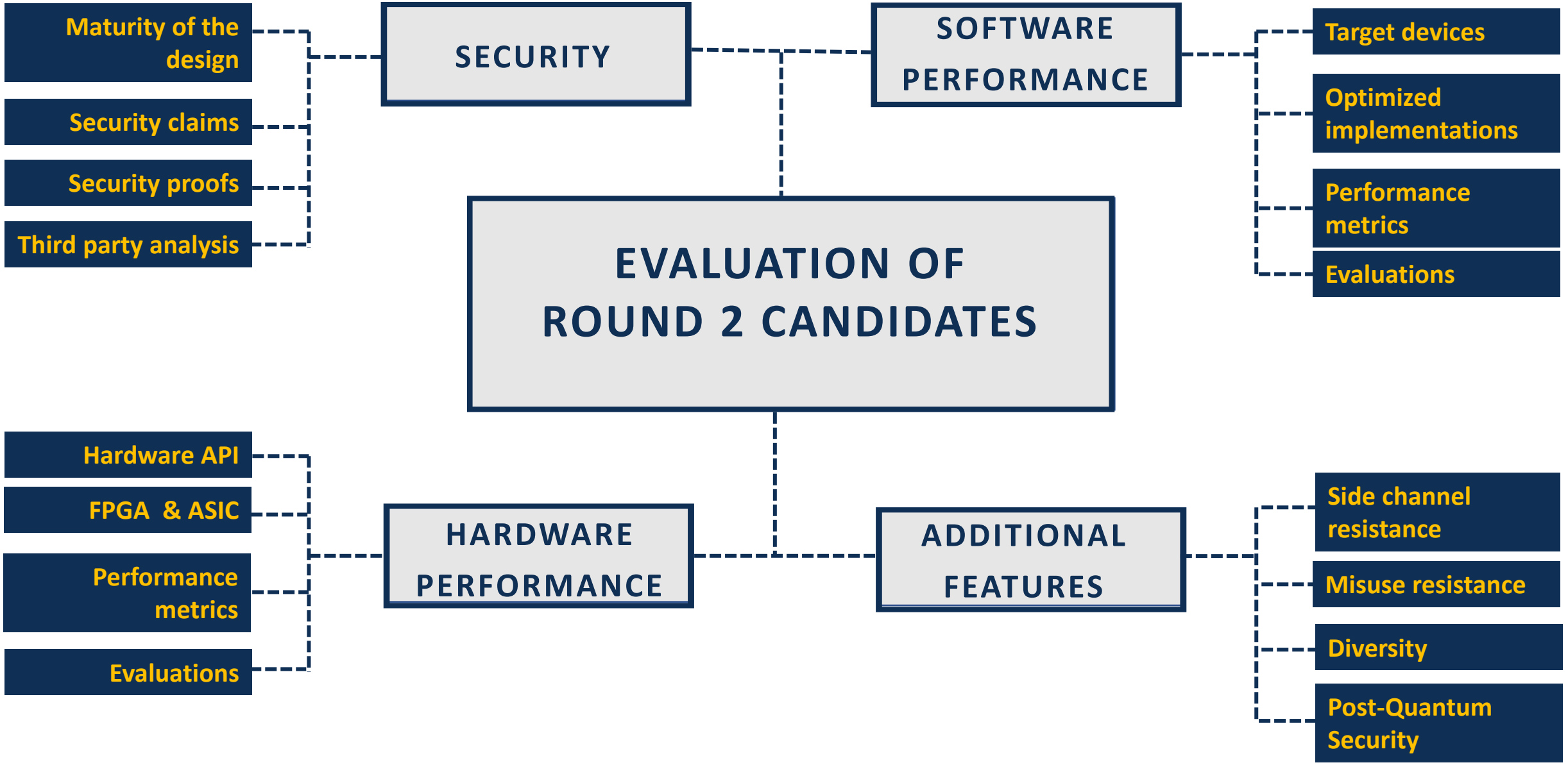
Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham

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

32 Round 2 Candidates

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


EVALUATION OF ROUND 2 CANDIDATES
SECURITY
Maturity of the design
Security claims
Security proofs
Third party analysis
SOFTWARE PERFORMANCE
Target devices
Optimized implementations
Performance metrics
Evaluations
HARDWARE PERFORMANCE
Hardware API
FPGA & ASIC
Performance metrics
Evaluations
ADDITIONAL FEATURES
Side channel resistance
Misuse resistance
Diversity
Post-Quantum Security

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

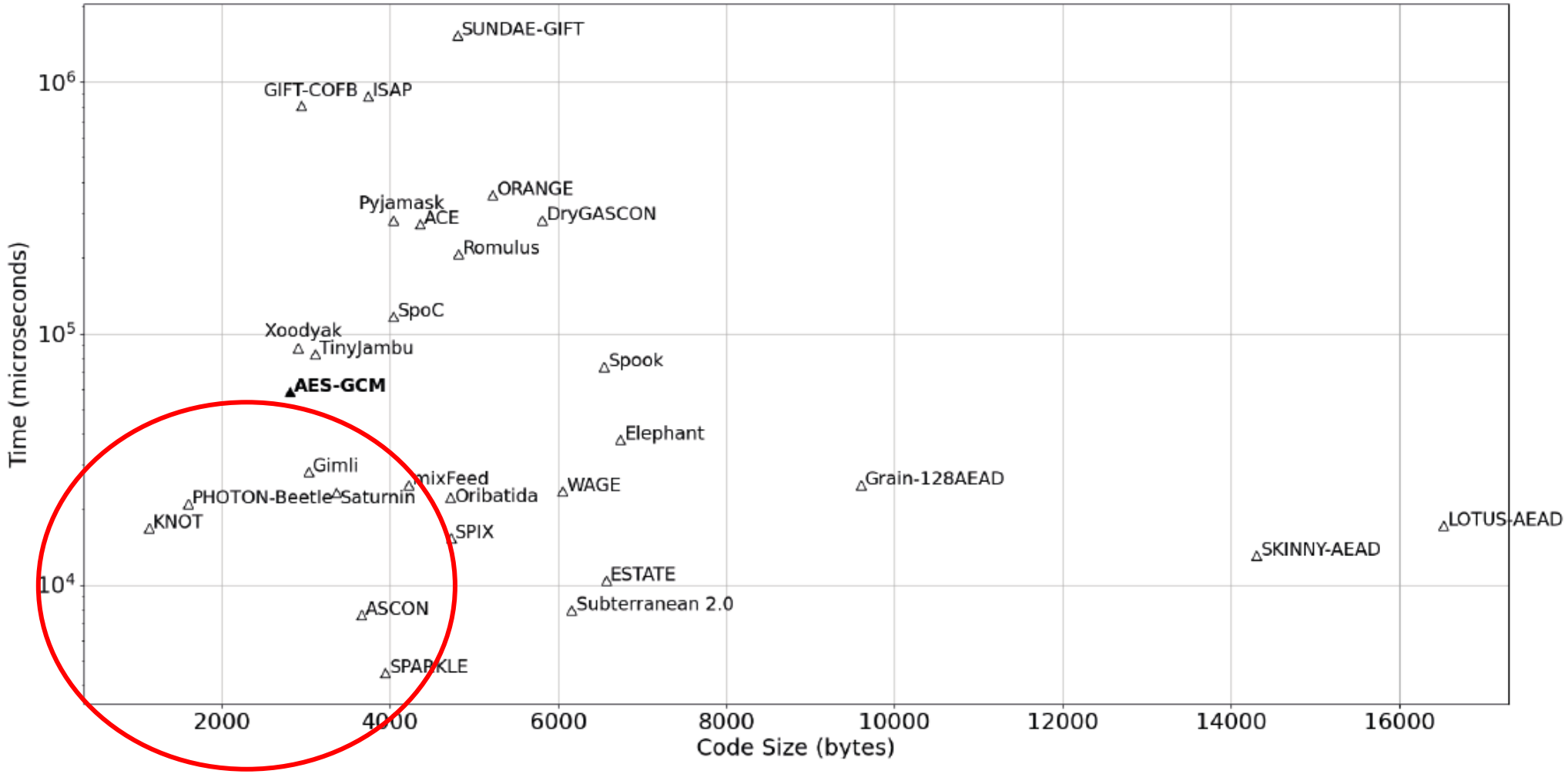
Metrics:
- Speed

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

Results – Software Benchmarking



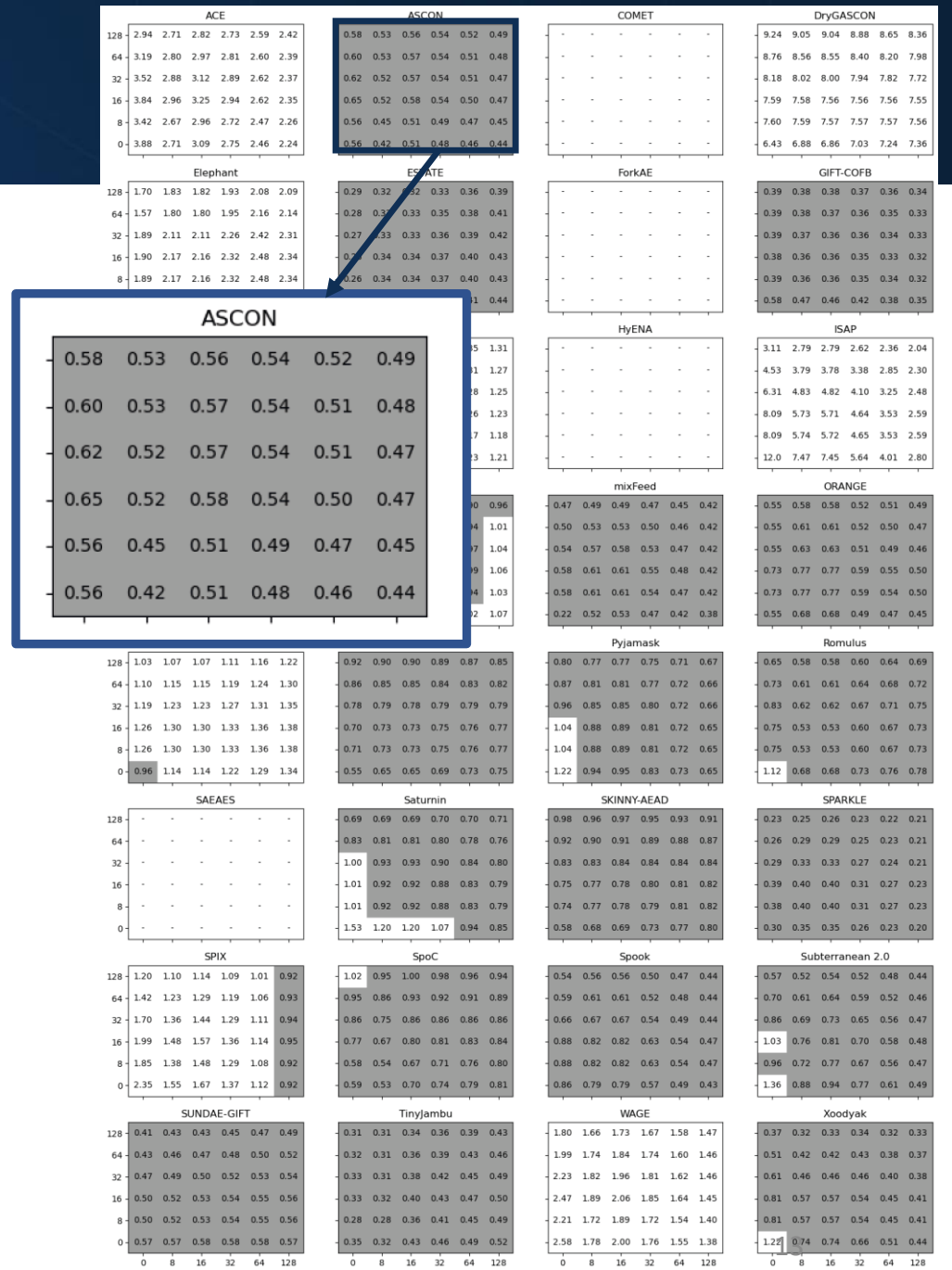
Code size vs. speed results of the smallest primary AEAD variants - 16-byte message and 16-byte AD on ATmega328P

Results – 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).

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



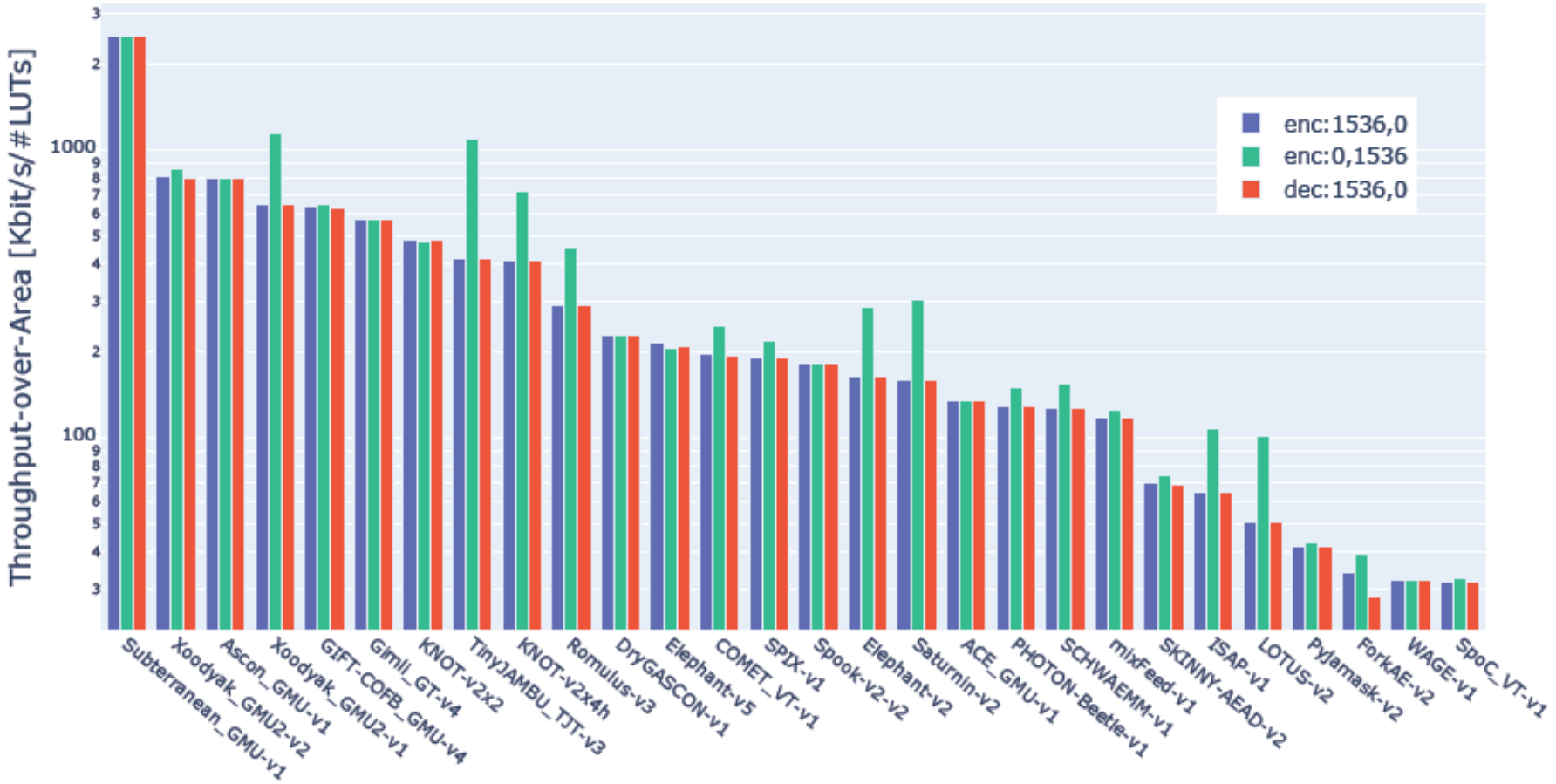
Result:

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)

Results – Hardware Benchmarking



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

Status Updates

In August 2020, NIST requested *optional* status updates from the submission teams on

- new proofs/arguments supporting the security claims
- new optimized/protected software and hardware implementations
- responds to third-party analysis
- 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 (out of 32) status updates.

Selecting the Finalist

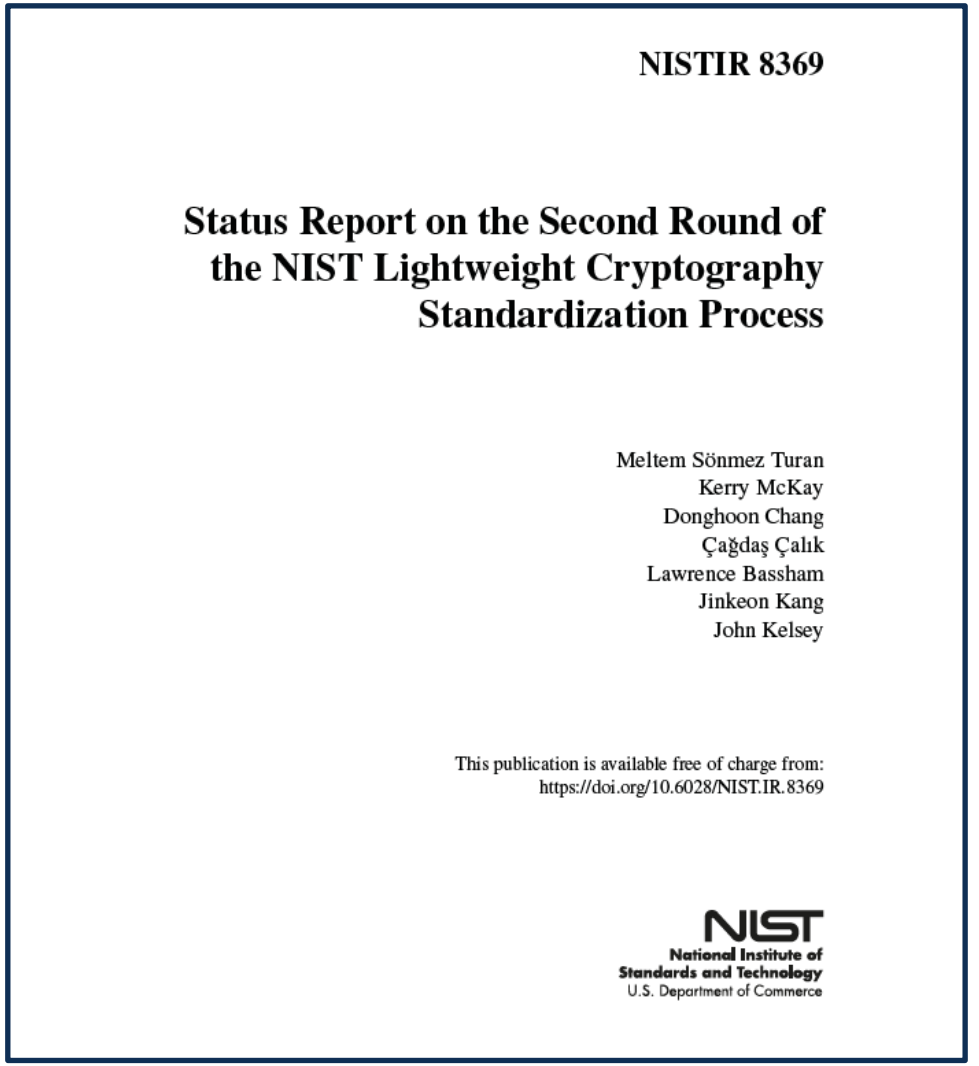
- Evaluation of the second-round candidates took around 20 months (from Aug. 2019 to March 2021).

Two workshops

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

In March 2021, NIST announced 10 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

New Submission Packages

- Finalists had the opportunity to update submission packages and propose tweaks to submissions.
- The tweaks included
  - Increasing/decreasing number of rounds
  - Adding new functionality (e.g., XOF, hash, new modes) and new variants
  - Dropping family members
  - Updating primary variants
  - Modifying the internal details of the underlying primitive

Timeline


1st Workshop
2nd Workshop
NISTIR 8114
Submission due
Round 1
Round 2
NISTIR 8268
3rd Workshop
4th workshop
Round 3
NISTIR 8369
5th Workshop
End of Round 3
July 2015
October 2016
March 2017
February 2019
April 2019
August 2019
October 2019
November 2019
October 2020
March 2021
July 2021
Spring 2022
Summer 2022

Next Steps

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