# On the Final Round of the NIST Lightweight Cryptography Standardization

Meltem Sönmez Turan
NIST Lightweight Cryptography Team

Security and Implementation of Lightweight Cryptography (SILC)
October 16, 2021 – Zagreb, Croatia

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

ITL INFORMATION TECHNOLOGY LABORATORY

Background

Evaluation of the Second-round Candidates

Final Round

Next Steps

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

INFORMATION TECHNOLOGY LABORATORY

# Background

## 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

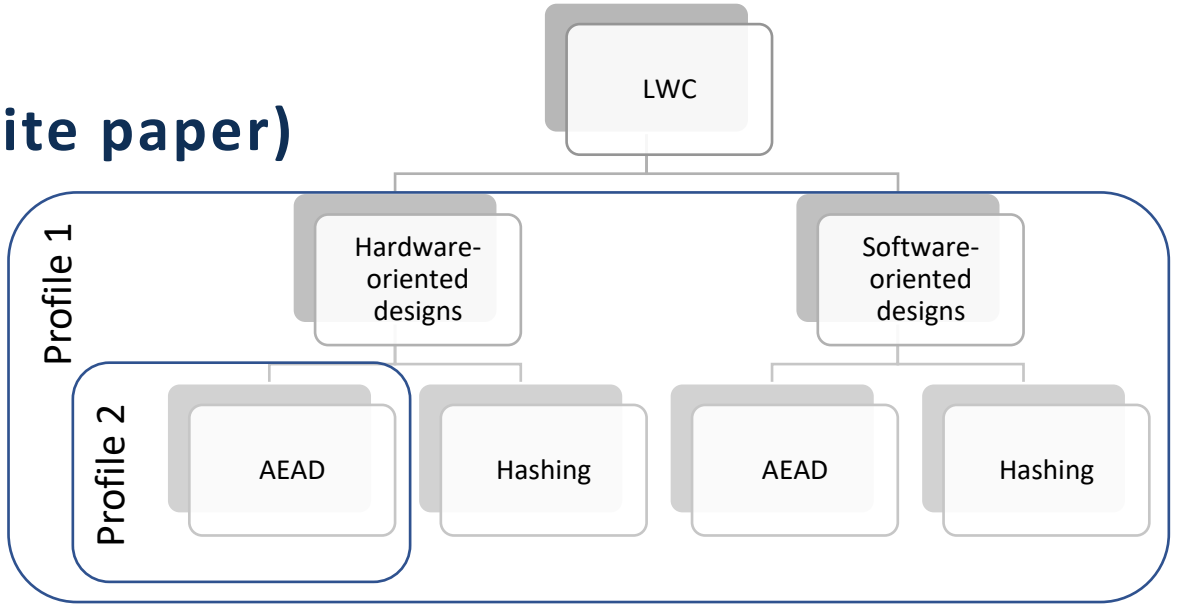
NIST crypto standards are optimized for general-purpose computers

# Early Feedback from Academia & Industry

- Two Lightweight Cryptography Workshops at NIST in July 2015 and October 2016.
- In March 2017, NISTIR 8114 Report on Lightweight Cryptography is published.

**Profiles for Lightweight Cryptography (white paper)**

- Profile I Authenticated Encryption with associated data (AEAD) and hashing for constrained software and hardware environments
- Profile II AEAD for constrained hardware environments



# Example Applications

**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**

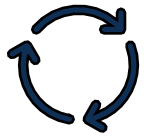
- Electrical home appliances with low-end CPUs
- Software-oriented primitives that consume less CPU time and smaller ROM requirements

## 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

**Single profile** 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

# Security 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

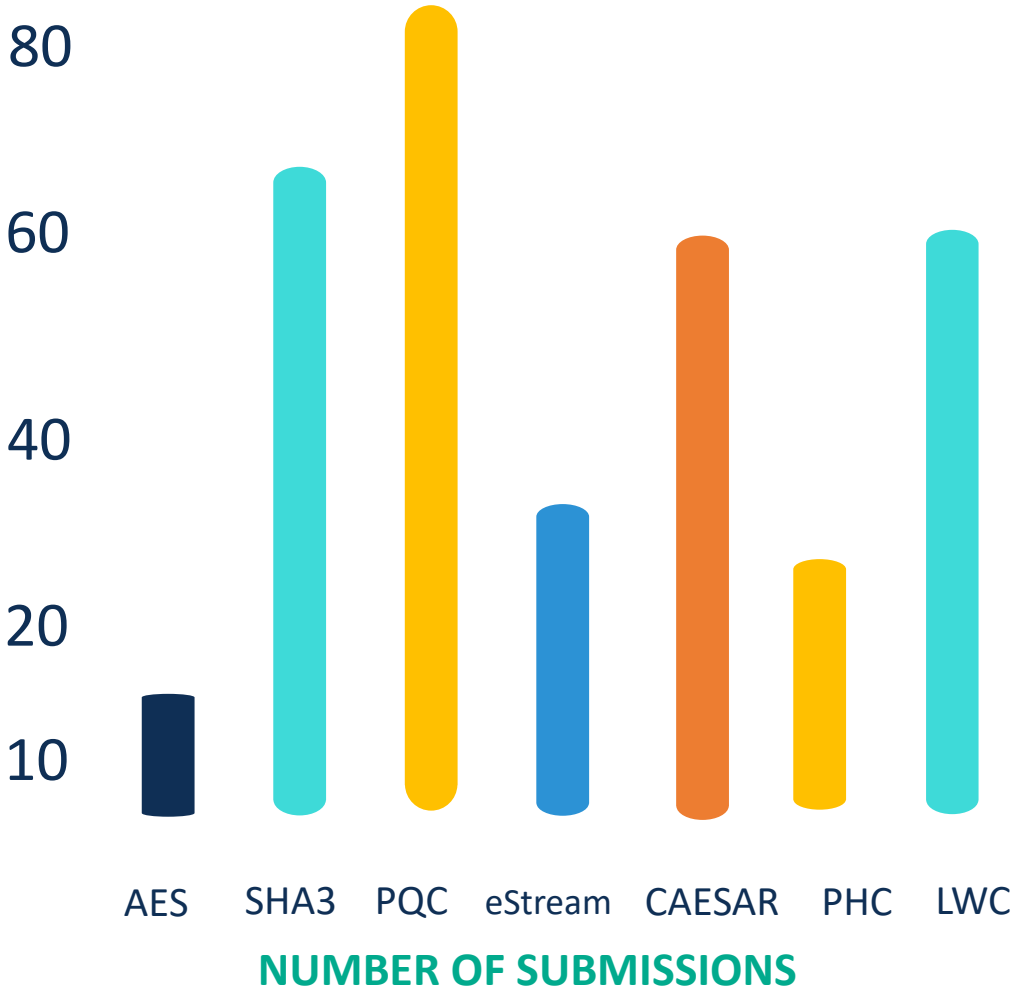
## Hash

- 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 $2^{50}$-1 bytes
- Common design components with the AEAD

# Design and Implementation Requirements

- Perform significantly better in constrained environments (HW and SW platforms) compared to NIST standards.
- Efficient for short messages
- Implementations that lend themselves to countermeasures against side channel attacks, and fault attacks

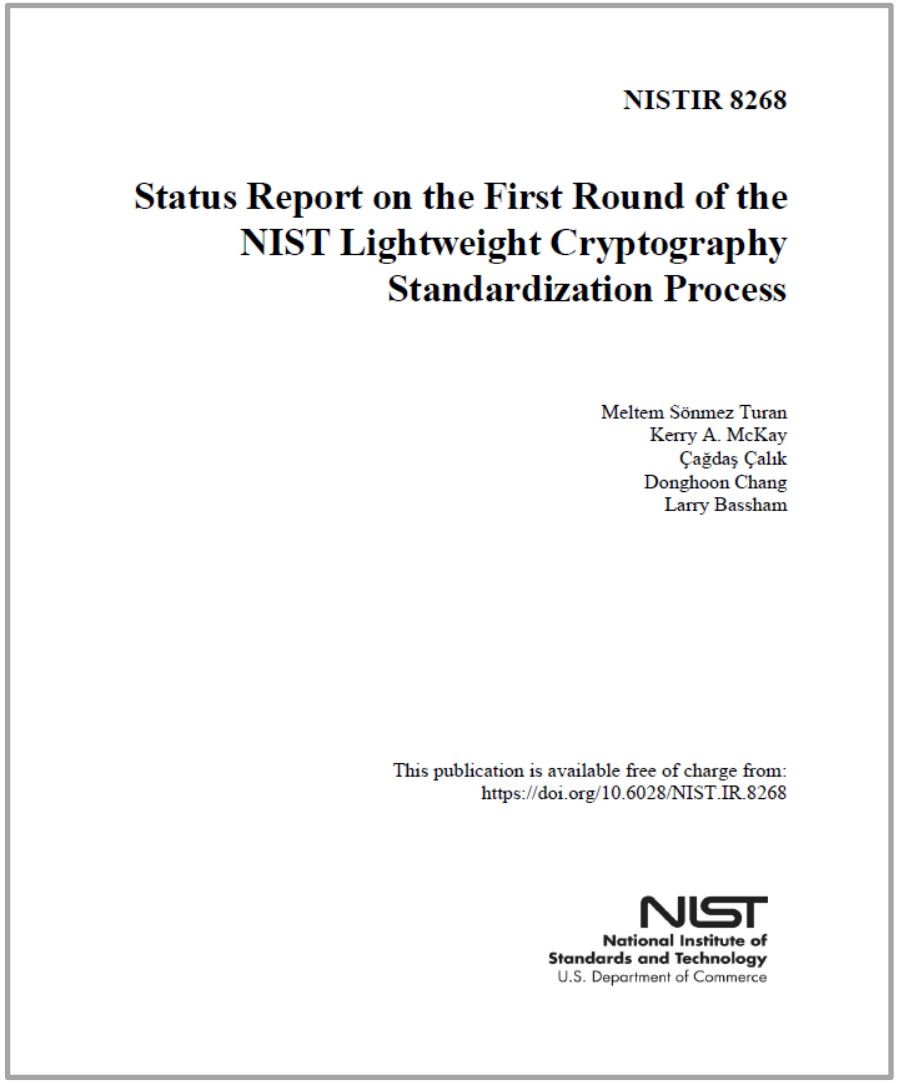
# 56 Round 1 Candidates





# First Round of the Standardization Process

- Approximately 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* (October 2019)



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

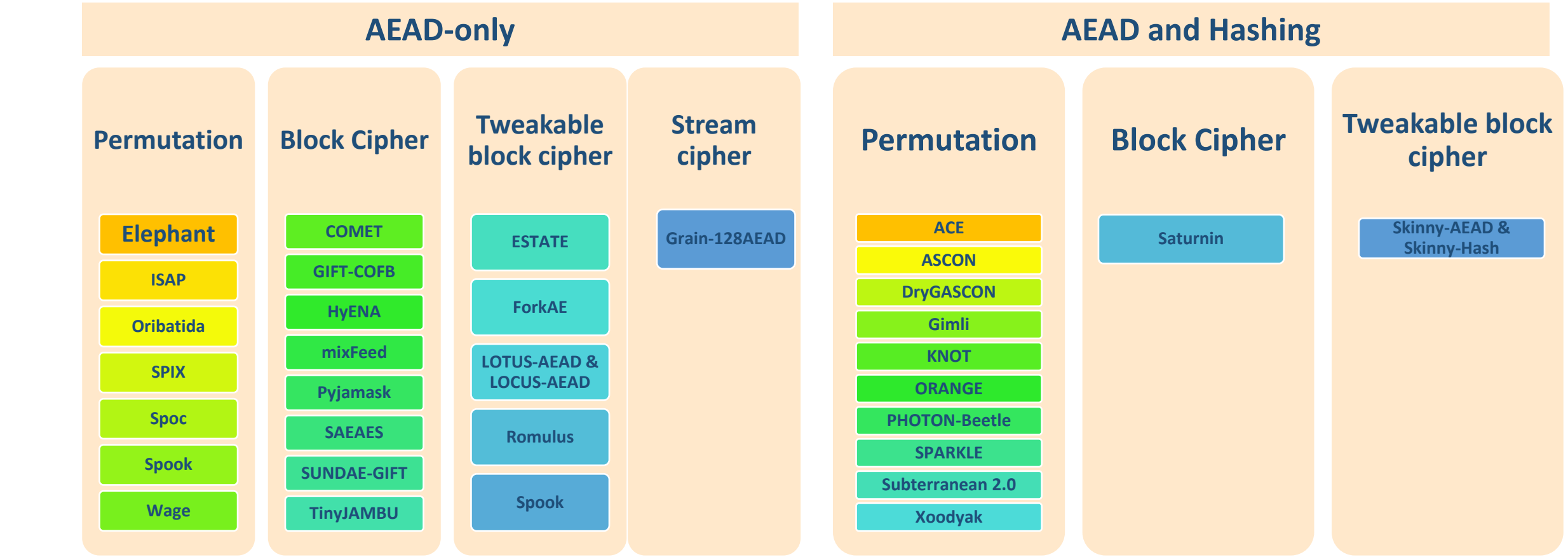
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

# The Second Round

# Second-Round Candidates

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

# Classification based on Underlying Components



# Classification based on Modes*

## 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

**Enc-then-Mac**

ISAP, Saturnin

**(T)BC-based Feedback with Rate 1**

COMET, GIFT-COFB, HyENA, mixFeed, Romulus

**Mac-then-Enc**

ESTATE, SUNDAE-GIFT

**Classical Sponge with Secret Permutation**

SAEAES, TinyJAMBU

**Stream Cipher Based**

Grain-128AEAD

## Parallel

ForkAE

LOTUS-AEAD & LOCUS-AEAD

**ΘCB3-based**

SKINNY-AEAD

**OCB3-based**

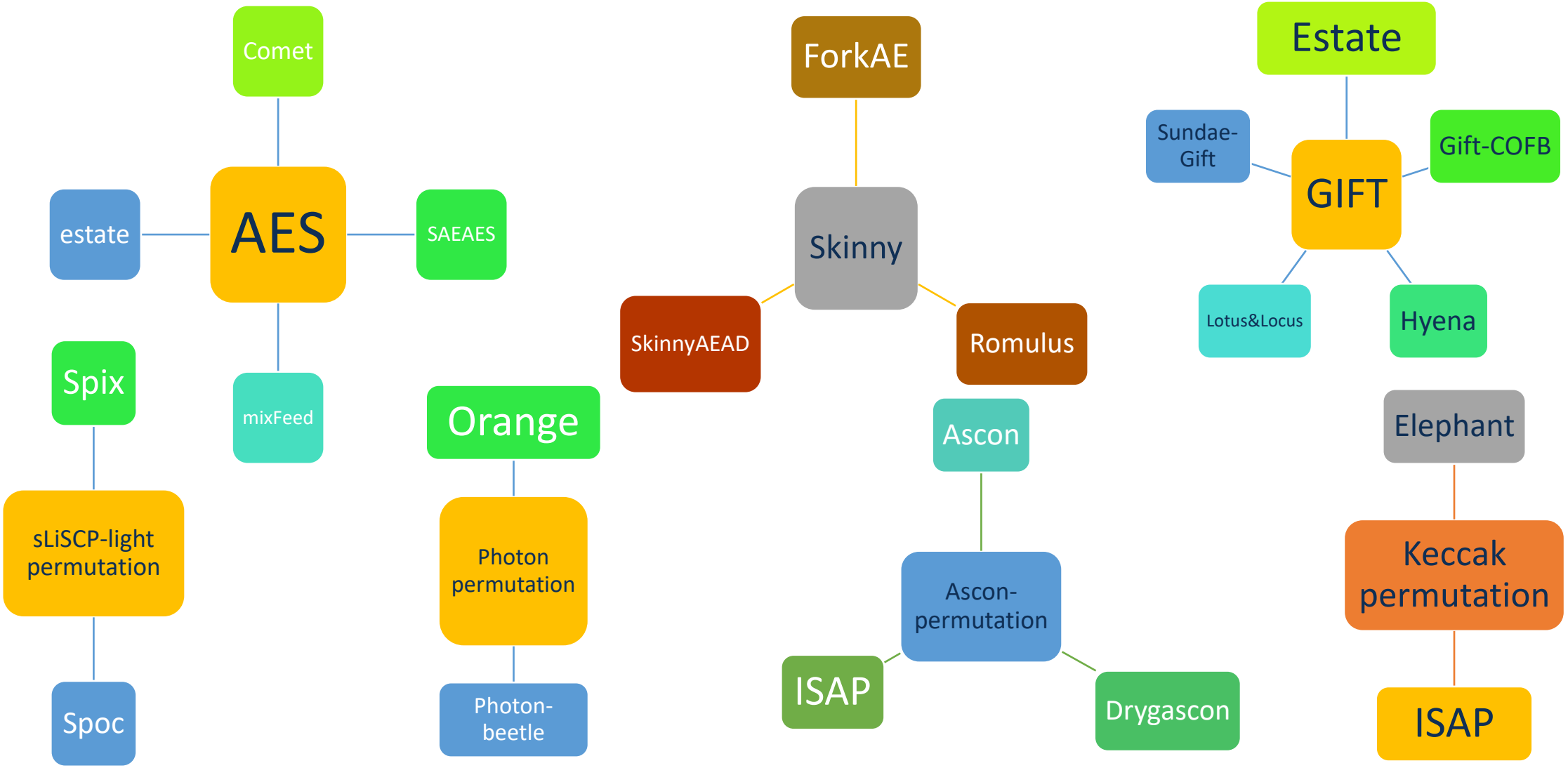
Pyjamask

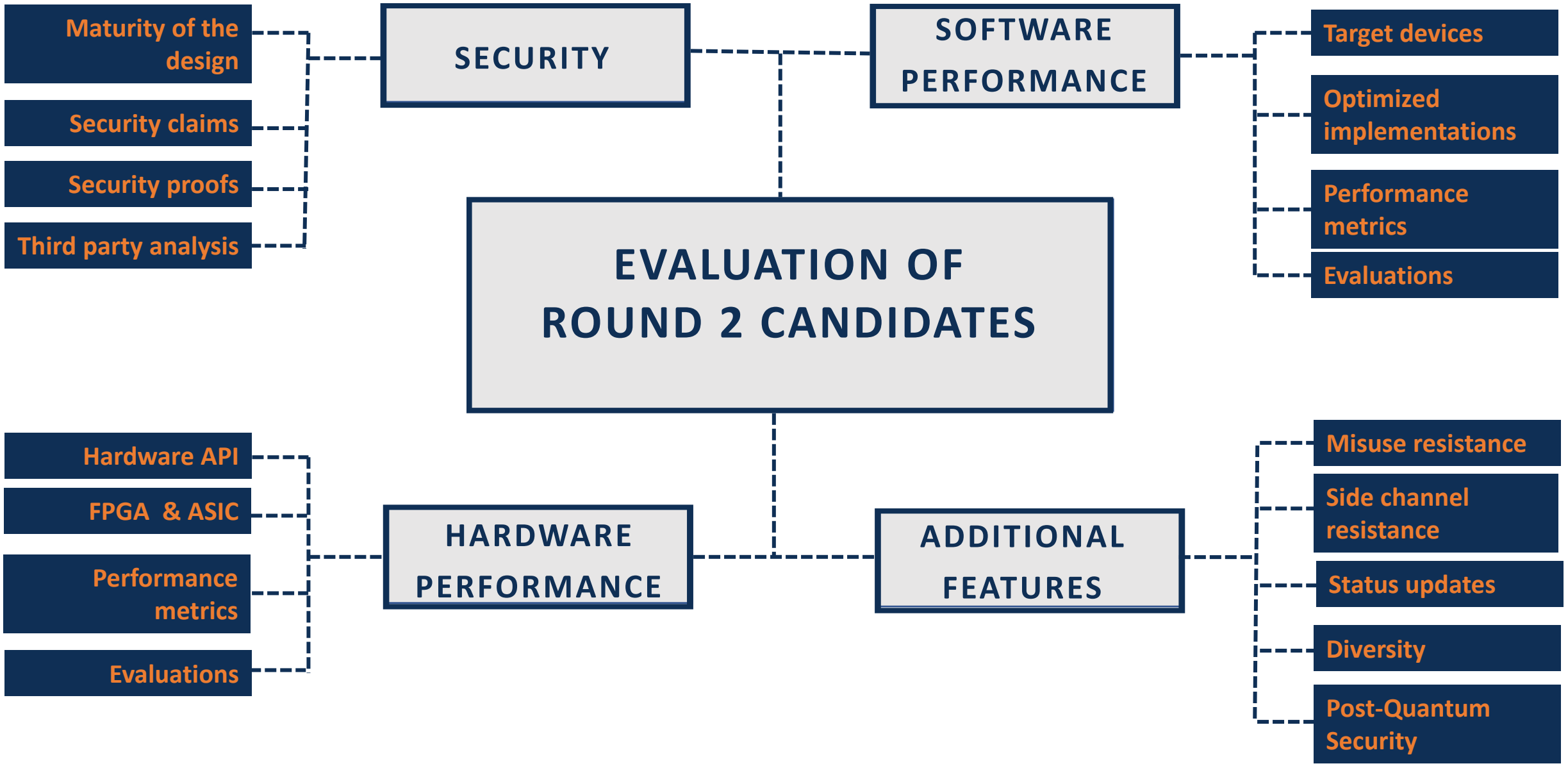
**Enc-then-Mac**

Elephant

* Primary variant only

# Common Building Blocks




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
Misuse resistance
Side channel resistance
Status updates
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

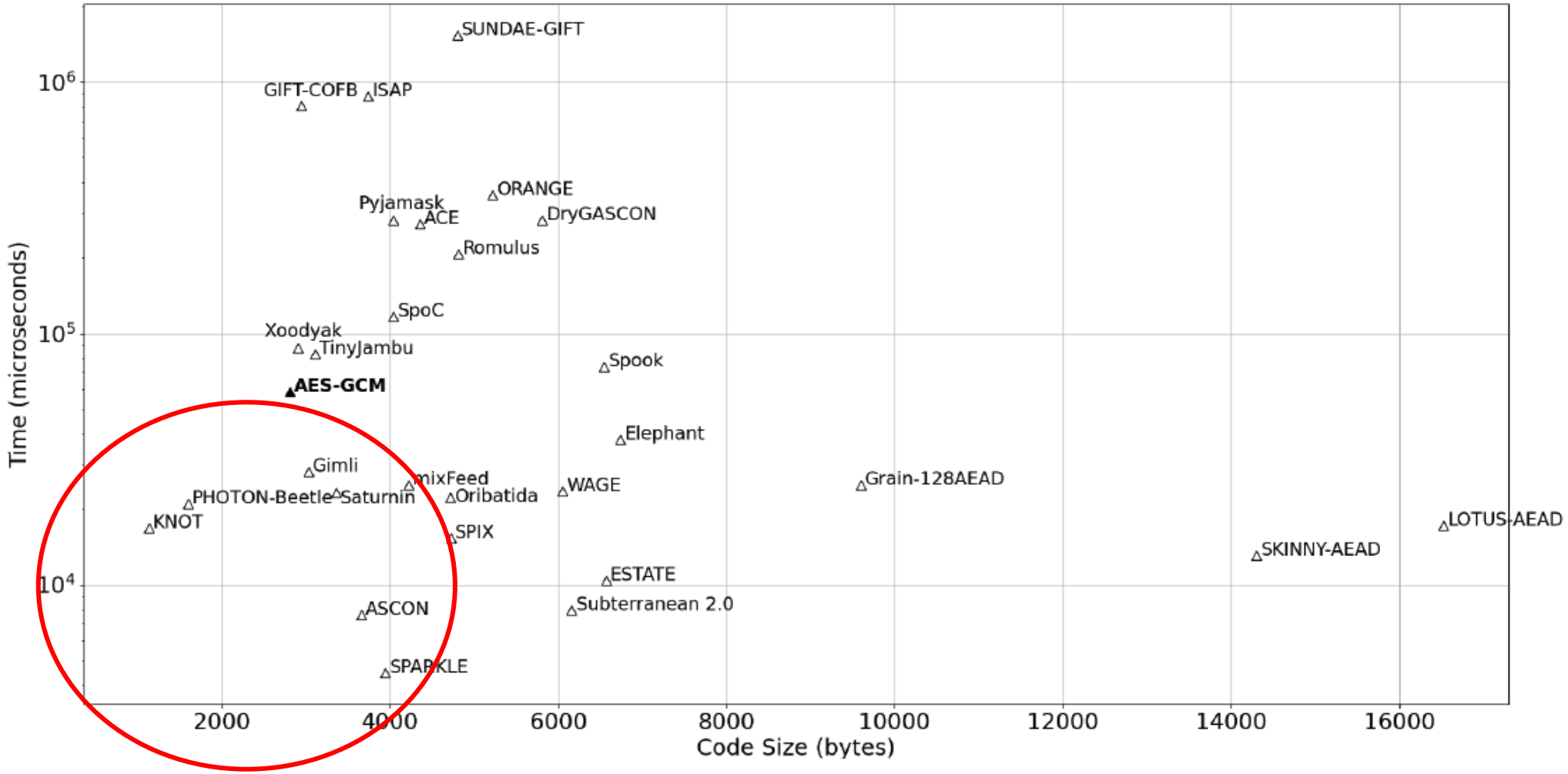
**Metrics:**
- Speed

**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



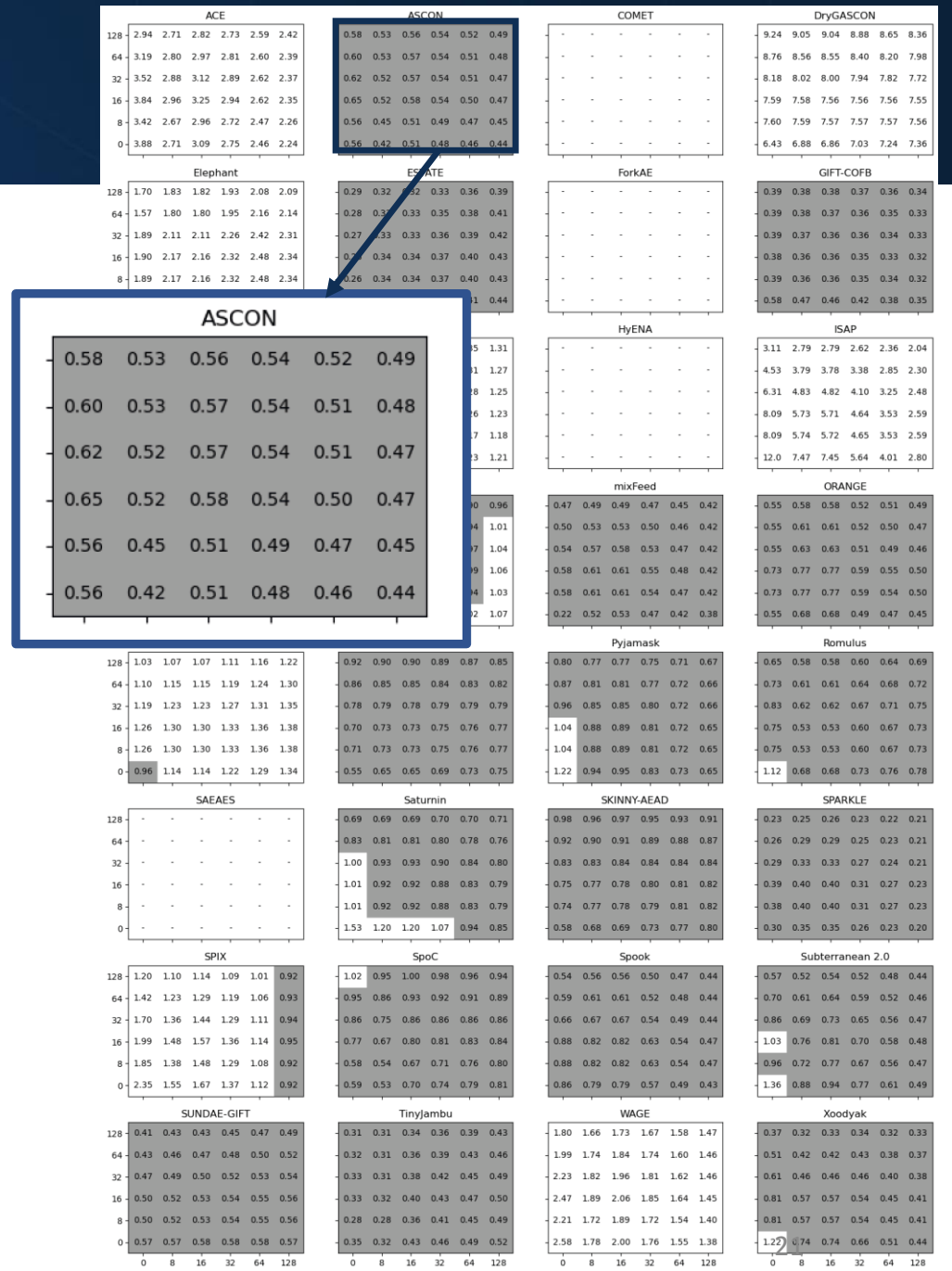

Code size vs. speed results of the smallest primary AEAD variants - 16-byte message and 16-byte AD on ATmega328P

# 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).

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



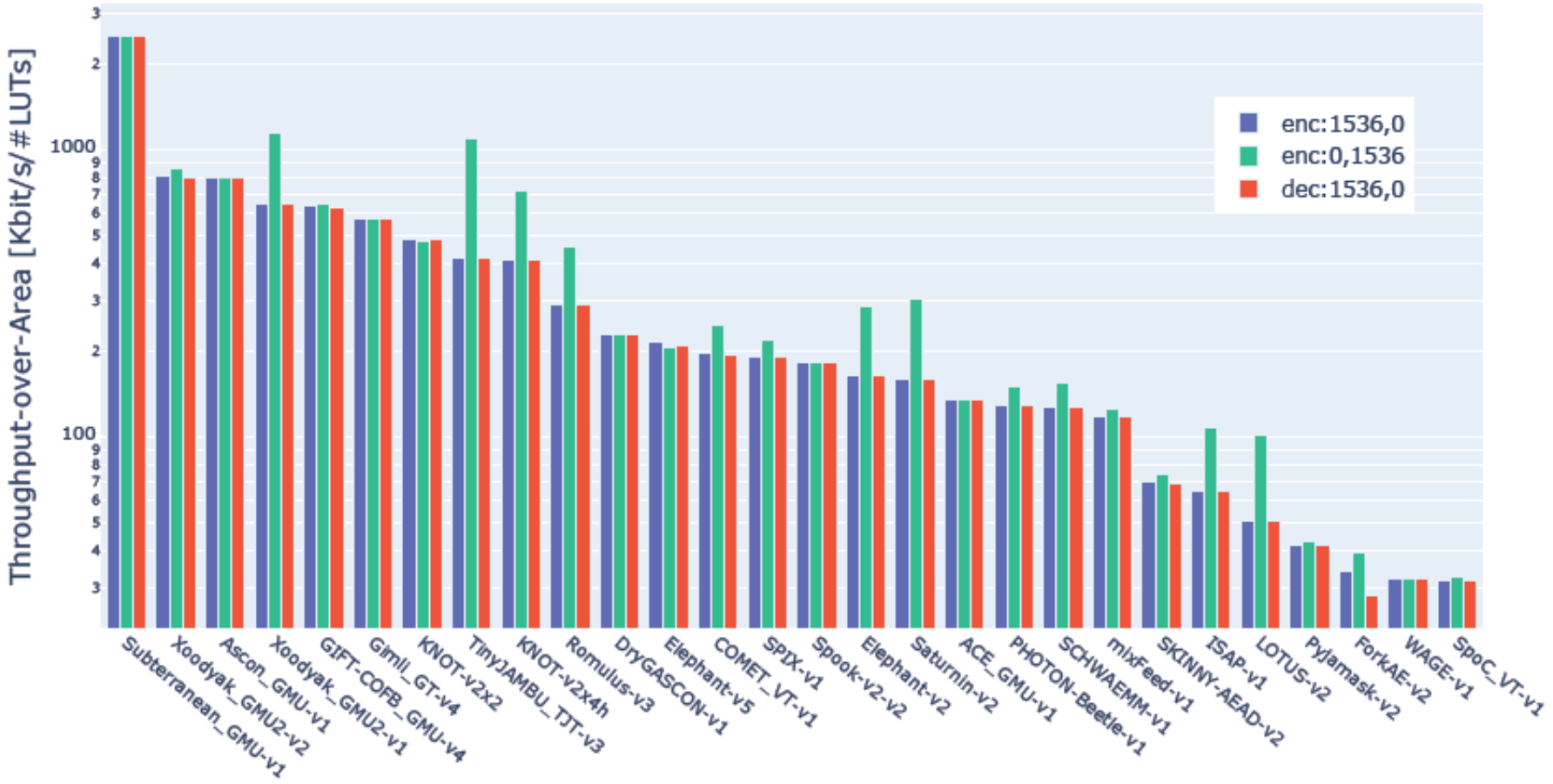

**Result:**

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<br>Intel Cyclone 10 LP<br>Lattice Semiconductor ECP5 | Resource utilization (LUT or LE, flip-flops)<br>Maximum clock frequency (MHz)<br>Throughput (Mbits/s)<br>Energy per bit (nJ/bit) |
| Khairallah et al. | TSMC 65nm<br>FDSOI 28nm | Area ($\mu m^2$ and GE)<br>Clock period (ns)<br>Power (mW)<br>Energy (mJ) |
| Aagaard and Zidarič | ST Micro 65nm<br>TSMC 65nm<br>ST Micro 90nm<br>TSMC 90nm<br>ARM/IBM 130nm | Throughput (bits per cycle)<br>Area (GE)<br>Energy (nJ)<br>Area×Energy (GE×nJ)<br>Clock Speed (GHz) |

# Results – Hardware Benchmarking




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

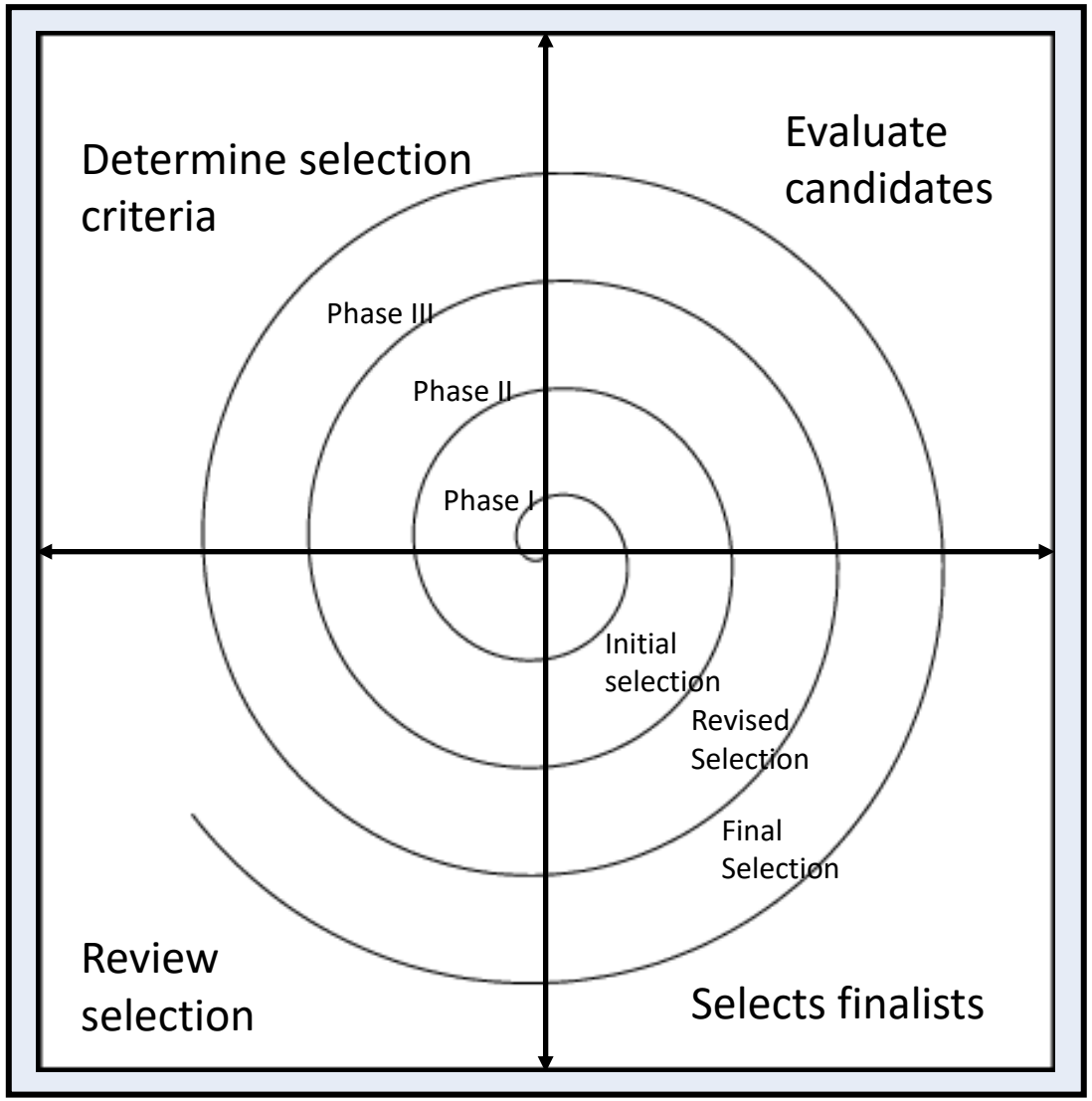
# Additional Features

- Nonce is assumed to be unique. Misuse resistance is a plus.
- Post quantum security is not included in the call.
  - Most symmetric-key algorithms are believed to be secure against quantum threats. Best generic attack: Grover's algorithm (quadratic speedup over exhaustive search)
  - Ascon, Gimli, Saturnin address the issue in their specification
  - Six candidates with large key sizes: DryGascon, Knot, SAEAES, Sparkle, Spook, TinyJambu.
- *Complexity of recovering the key from the internal state* is not mentioned in the call.
  - Keyed initialization and finalization makes it hard to recover the key.
- Status updates and the tweak plans were also considered.
  - e.g., Increasing/decreasing number of rounds, new functionality, internal changes
- Diversity of the finalists + current NIST standards

# Challenges of Evaluation

- **Large number of candidates:**
  - 32 family of algorithms (89 AEAD, 19 hash variants). Evaluation mostly done on *primary variants.*
- **Limited resources:**
  - Mostly relies on third-party analysis.
  - Not all algorithms get the same attention.
- The industry need is not clear.
  - too specific vs. too broad
- **Assigning weights for different criteria:**
  - Different security claims (nonce misuse, RUP security, side channel resistance, etc.), different functionality (AEAD, hash, XOF etc.), attacks with different complexities

# Evaluation strategy



# Selecting the Finalist

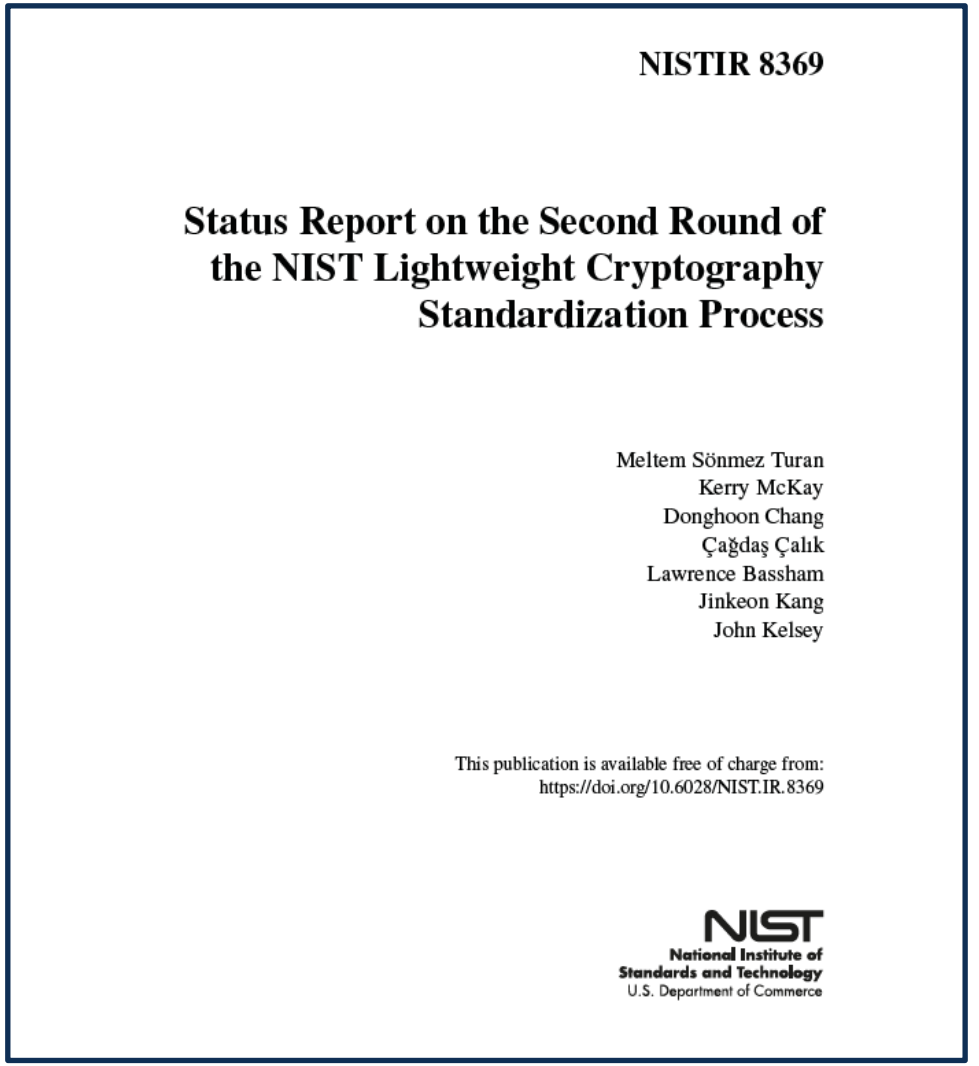
- Evaluation of the second-round candidates took around 20 months (from Aug. 2019 to March 2021).

Two workshops

- Nov. 2019 – Third LWC Workshop
- Oct. 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

| Finalist | Building Block | Mode | #variants | Key size | Nonce size | Tag size |
|---|---|---|---|---|---|---|
| Ascon | Permutation | Monkey dublex | 3 aead<br>4 hash | 128-160 | 128 | 128 |
| Elephant | Permutation | Enc-then-MAC | 3 aead | 128 | 96 | 64-128 |
| Gift-COFB | Block cipher | Combined feedback | 1 aead | 128 | 128 | 128 |
| Grain-128aead | Stream cipher | - | 1 aead | 128 | 96 | 64 |
| ISAP | Permutation | Enc-then-MAC | 4 aead | 128 | 128 | 128 |
| Photon-beetle | Permutation | Combined feedback | 2 aead<br>1 hash | 128 | 128 | 128 |
| Romulus | Tweakable BC | Mac-then-Enc | 3 aead<br>1 hash | 128 | 128 | 128 |
| Sparkle | Permutation | Duplex | 4 aead<br>2 hash | 128-256 | 128-256 | 128 |
| TinyJambu | Keyed Permutation | Duplex | 3 aead | 128-256 | 96 | 64 |
| Xoodyak | Permutation | Cyclist | 1 aead<br>1 hash | 128 | 128 | 128 |

# Next Steps

- Evaluation of the finalists
- Fifth Lightweight Cryptography Workshop(~May 9-11, 2022)
- Selection of the winner(s) and publication of the report
- Standardization

# 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

# 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

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

ITL INFORMATION TECHNOLOGY LABORATORY