Towards the Selection of the Finalists

NIST Lightweight Cryptography Standardization Process

Kerry McKay
NIST Lightweight Cryptography Team

NIST Lightweight Cryptography Workshop, October 19, 2020

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

INFORMATION TECHNOLOGY LABORATORY

Outline

- NIST lightweight cryptography standardization process
- Comparisons of the round 2 candidates
- Evaluation criteria and next steps

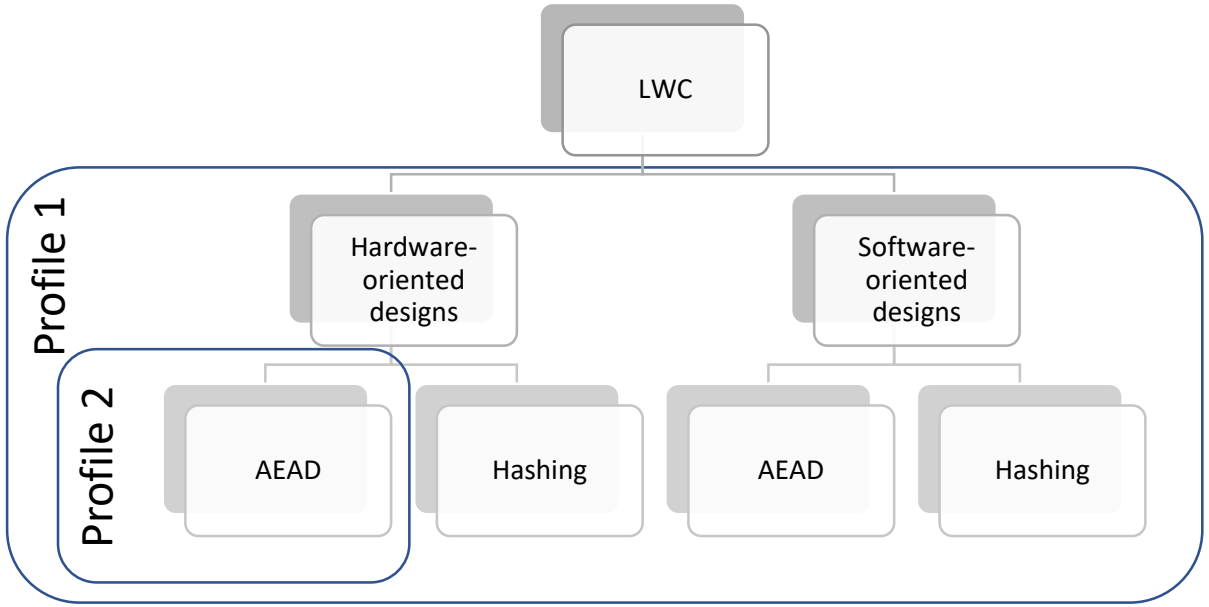
Welcome – 4th NIST LWC Workshop

- Three-day virtual workshop
- Six sessions to discuss
  - Status updates
  - Security analysis and performance of second round candidates
  - Selection of the finalists
- 2 NIST talks, 23 accepted talks, open discussion

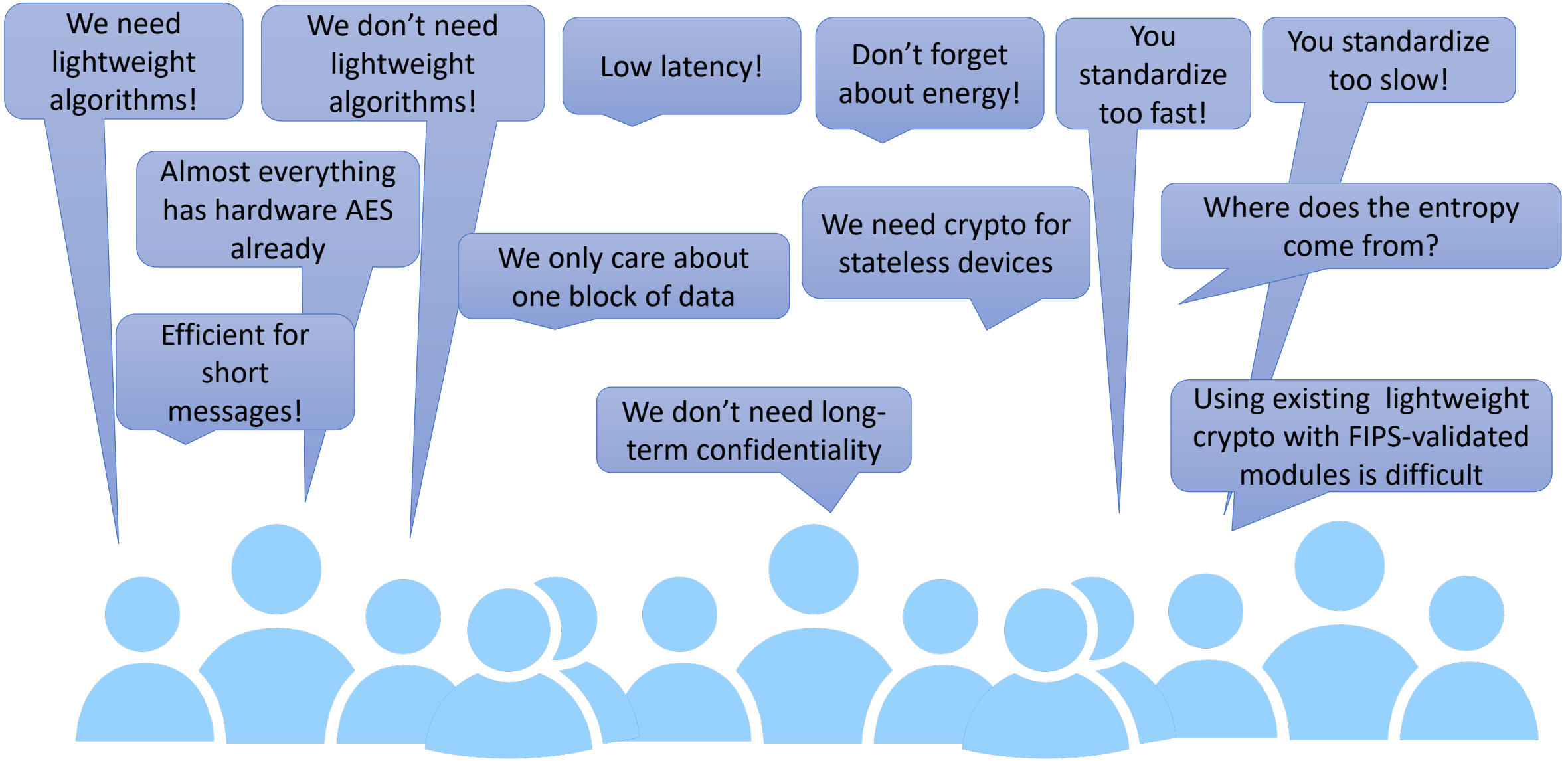
Where We Began

- Need for cryptographic standards for applications in constrained environment that are not well-served by existing NIST standards
  - Needs vary by application
  - Tailoring to target devices and applications could lead to many standards
- The big question was “where do we start?”
  - Decided to begin with symmetric cryptography in constrained environments

- Two profiles in withdrawn draft whitepaper
  - Profile 1 for AEAD + hashing in SW and HW
  - Profile 2 for AEAD in hardware
- Feedback shaped the submission requirements
- Instead of two profiles, asked for AEAD with optional hashing functionality

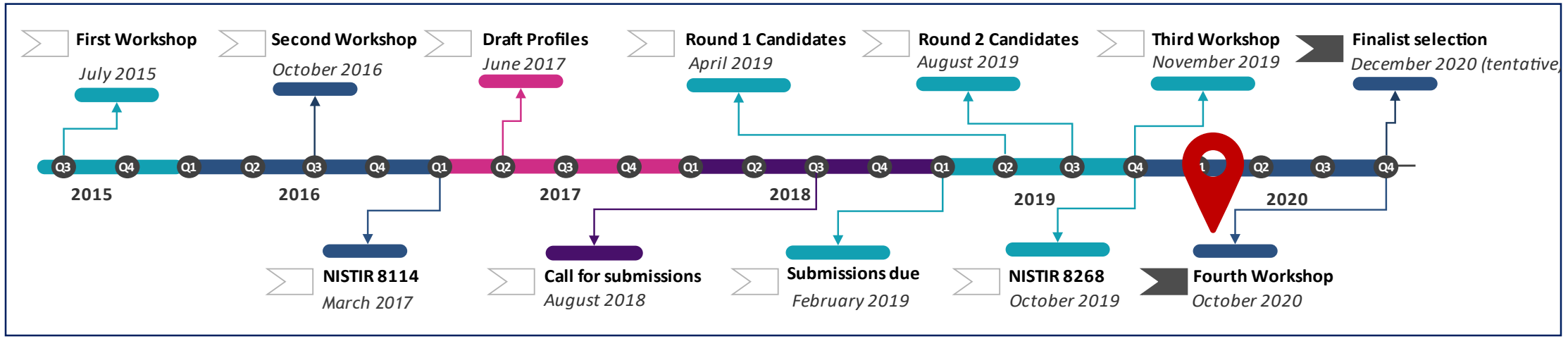


Feedback (paraphrased)



NIST LWC Standardization Process

- Competition-like process
- **Scope:** AEAD with optional hashing functionality
- In April 2019, announced 56 Round 1 candidates (out of 57 submissions)
- In August 2019, announced 32 Round 2 candidates
  - Selection based on cryptographic maturity of the designs
- Extended the finalist selection by 3 months, expected in December 2020

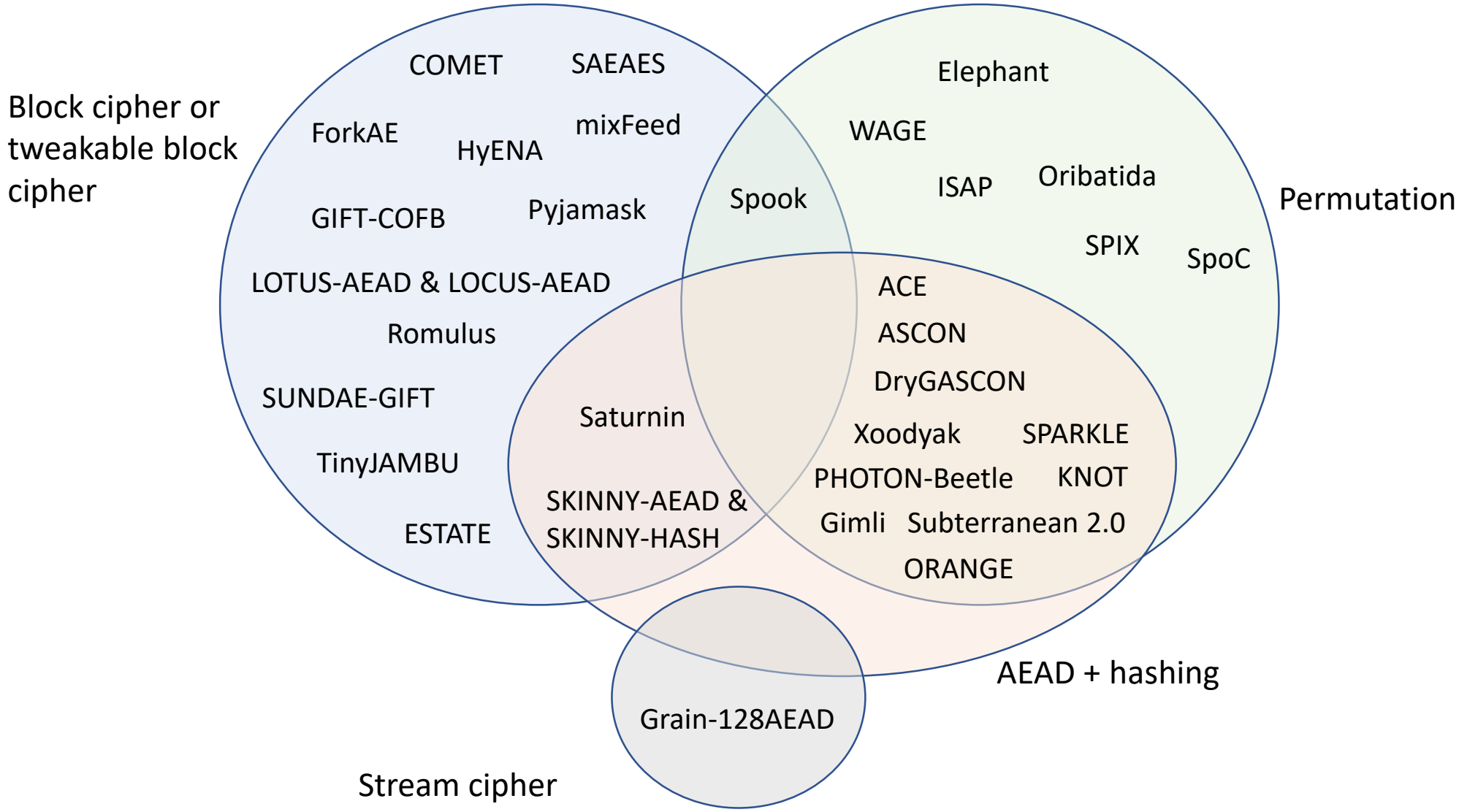


Considerations

- Security
  - Claims by the submitters
  - Maturity of analysis by the submitters and third parties
- Implementation flexibility to achieve cost/performance tradeoff best for application
- Performance
  - Benchmarking results in constrained software and hardware environments
  - Comparison to current NIST standards
- Additional Features
  - Nonce misuse security, RUP security, post-quantum security, side channel resistance, etc.
- Design diversity
- Standardization
  - Public confidence
  - Ease of standardization and adoption

Second Round Candidates

Design (Primitive Level) & Functionality



Design (Mode Level)*

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

(T)BC-based feedback with rate 1

COMET, GIFT-COFB, HyENA, mixFeed, Romulus

Classical sponge with secret permutation

SAEAES, TinyJAMBU

Enc-then-Mac

ISAP, Saturnin

Mac-then-Enc

ESTATE, SUNDAE-GIFT

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

Candidates Using Crypto Standards

AES (FIPS 197)	KECCAK (FIPS 202)	PHOTON (ISO/IEC 29192-5)	SKINNY** (ISO/IEC 18033-7)	SPONGENT (ISO/IEC 29192-5)
Comet	Elephant*	ORANGE	ForkAE*	Elephant
ESTATE*	ISAP*	PHOTON-Beetle	Romulus	
mixFeed*			SKINNY-AEAD/HASH	
SAEAES				

* with modification

** in progress

Additional Features

Many candidates claim additional features, such as

- Various levels of nonce misuse resistance
- RUP-security
- Related-key security
- Lending themselves to side-channel resistant implementations
  - Leakage-resilience, threshold implementations, etc.
- Post-quantum security
- Additional variants supporting various key/tag sizes, or optimization for short messages

Software Benchmarking

Microcontroller benchmarking by Renner, Pozzobon, and Mottok
• ATmega328P • ARM Cortex-M3 • ARM Cortex-M7 with FPU • Kendryte K210 • Xtensa LX6

Microcontroller benchmarking by Weatherley
• ARM Cortex-M3 • Xtensa LX6 • ATmega2560

Microcontroller benchmarking by NIST LWC Team
• ATmega328P • ARM Cortex-M0+ • ARM Cortex-M4 with FPU

eBACS (ECRYPT Benchmarking of Cryptographic Systems)
• Many systems covering ARM, AMD, Intel, PPC, RISC-V, and MIPS architectures

RISC-V benchmarking by Campos et al.
• SiFive E31 • VexRiscv simulator • riscvOVPsim simulator

Hardware Benchmarking

FPGA benchmarking by Mohajerani et al.	**ASIC benchmarking by Khairallah, Peyrin, and Chattopadhyay**
• Artix-7 • Cyclone 10 LP • ECP5	• Synopsys VCS simulator • Xilinx ISim simulator

Status Updates

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

- New proofs/arguments supporting the security claims
- New software and hardware implementations
- New third-party analysis and its implications
- 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
- Any other relevant information

NIST received 27 status updates

- Available on the project website at https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates

Tweaks

- Finalists will have the opportunity to update submission packages and propose tweaks to submissions.
- 15 teams are considering tweaking their submissions, according to status updates
  - Increasing/decreasing number of rounds
  - Adding new functionality (e.g., XOF, hash, new modes) and new variants
  - Swapping ordering of nonce/ad/message processing
  - Updating primary variants, input sizes (nonce size)
  - Dropping family members
  - Modifying the internal details of the underlying primitive
- Tweaks are expected to be small changes to the design
  - 'big' changes to the **primary variant** may signal that the submission is not mature enough for standardization
- Tweak submission guidelines will be provided

Finalist Selection

- After the 15-month evaluation of the second-round candidates, NIST plans to select the finalists in December
- Target around 8
- Selection criteria
  - Security analysis (third-party and submitter)
  - Software and hardware benchmarking
  - Diversity of the finalists
  - Additional features

Timeline and Next Steps

- Selection of the finalists
- Publication of the report on 2nd round
- Provide guidelines for the tweaks
- Deadline for updated submission packages
- Publication of the updated submissions in the project webpage

- Final round around one year

Thanks!

https://csrc.nist.gov/Projects/lightweight-cryptography

Email list: lwc-forum@list.nist.gov
NIST team: lightweight-crypto@nist.gov