On the NIST Lightweight Cryptography Standardization

Meltem Sönmez Turan
NIST Lightweight Cryptography Team

ECC 2019: 23rd Workshop on Elliptic Curve Cryptography
December 2, 2019

Outline

- NIST's Cryptography Standards
- Overview - Lightweight Cryptography
- NIST Lightweight Cryptography Standardization Process
- Announcements

NIST's Cryptography Standards

National Institute of Standards and Technology

- Non-regulatory federal agency within U.S. Department of Commerce.
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988.
- Headquarters in Gaithersburg, Maryland, and laboratories in Boulder, Colorado.
- Employs around 6,000 employees and associates.

NIST's 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.

NIST Organization Chart

Laboratory Programs

- Center for Nanoscale Science and Technology
- Communications Technology Lab.
- Engineering Lab.
- **Information Technology Lab.**
- Material Measurement Lab.
- NIST Center for Neutron Research
- Physical Measurement Lab.

Information Technology Lab.

- Advanced Network Technologies
- Applied and Computational Mathematics
- Applied Cybersecurity
- **Computer Security**
- Information Access
- Software and Systems
- Statistical Engineering

Computer Security Division

- Cryptographic Technology
- Secure Systems and Applications
- Security Outreach and Integration
- Security Components and Mechanisms
- Security Test, Validation and Measurements

Computer Security Division (CSD)

Conducts research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect nation's information and information systems.

CSD Publications

- Federal Information Processing Standards (FIPS): Specify approved crypto standards.
- NIST Special Publications (SPs): Guidelines, technical specifications, recommendations and reference materials, including multiple sub-series.
- NIST Internal or Interagency Reports (NISTIR): Reports of research findings, including background information for FIPS and SPs.
- NIST Information Technology Laboratory (ITL) Bulletins: Monthly overviews of NIST's security and privacy publications, programs and projects.

Standard Development Process

- International "competitions": Engage community through an open competition (e.g., AES, SHA-3, PQC, Lightweight Crypto).
- Adoption of existing standards: Collaboration with accredited standards organizations (e.g., RSA, HMAC).
- Open call for proposals: Ongoing open invitation (e.g., modes of operations).
- Development of new algorithms: if no suitable standard exists (e.g., DRBGs).

Principles: Transparency, openness, balance, integrity, technical merit, global acceptability, usability, continuous improvement, innovation and intellectual property

More info: NISTIR 7977 NIST Cryptographic Standards and Guideline Development Process, 2016

NIST-Approved Crypto Standards (NIST SP 800 131A)

Block Ciphers

- Triple DES*(SP 800-67), SKIPJACK*(FIPS 185), AES (FIPS 197)

Modes of Operation (SP 800 38 series)

- ECB, CBC, CFB, OFB, XTS-AES, CCM, GCM, FF1, FF3, etc.

Hash Functions

- SHA-1*, SHA-2 (FIPS 180), SHA-3 (FIPS 202), TupleHash and ParallelHash (SP 800-185)

MAC

- CMAC, GMAC (based on block ciphers), HMAC, KMAC (based on hash functions)

Digital signatures

- DSA, ECDSA, RSA (new updates)

Other standards

- Key agreement, key derivation, random bit generation etc.

NIST museum https://www.nist.gov/nist-museum/about

Lightweight Cryptography

Motivation

Shift from general-purpose computers to dedicated resource-constrained (with limited processing and storage capabilities) devices such as RFID tags, sensor networks, IoT devices

Some Applications

RAIN RFID anti-counterfeiting

- Counterfeiting can be avoided by authenticating the tags using a challenge-response protocol.
- 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 requirement

Automobiles

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

Medical Sensors

- Measuring blood pressure, blood sugar etc.
- Hardware-oriented primitives with low power consumption

Smart Home Appliances

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

📷: NIST Net-zero House by Beamie Young/NIST

Lightweight Cryptography (LWC)

Subfield of cryptography that aims to provide crypto solutions optimized for constrained environments.

- Many iterations of simple rounds, simple operations (e.g., 4x4 Sboxes, bit permutations), simpler key schedules etc.

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

Hardware applications:

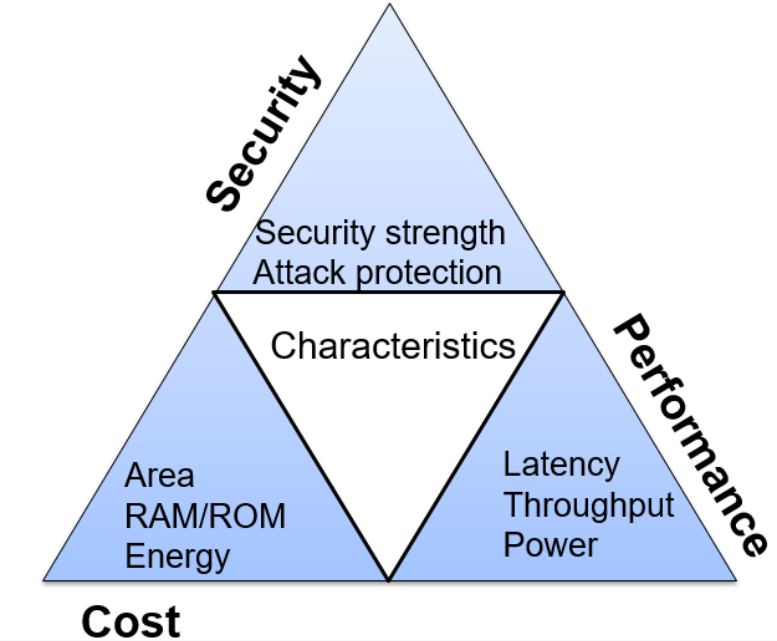
- Area, latency, throughput, power consumption etc.

Software applications:

- RAM, code size, throughput etc.

📷: The International Prototype Kilogram, aka Le Grand K. Credit: BIPM

Tradeoff between Security, Cost and Performance



Challenge: Optimal tradeoff depends on the target technology and application. Due to the variability of applications/requirements, hard to select a one-size-fits-all algorithm.

LWC Initiatives and Standards

Lightweight Cryptography standards/proposals by

- eSTREAM: A 4-year network of excellence funded project started in 2004 by European Network of Excellence for Cryptology (ECRYPT)
- CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness
- CRYPTREC: Cryptography Research and Evaluation Committees set up by the Japanese Government
- ISO/IEC: International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC)

LWC Initiatives and Standards - eSTREAM (2004-2008)

Goal: To identify new stream ciphers that might be suitable for widespread adoption and to stimulate work in stream ciphers.

- for software applications with high throughput requirements with key size of 256 bits, and
- **for hardware applications with restricted resources with key size of 80 bits.**

Finalists for hardware applications:

- Grain: Widely analyzed, updated version featuring authentication
- Trivium: Widely analyzed, simple and elegant, only has 80-bit version
- MICKEY: hard to analyze, less implementation flexibility, due to irregular clocking, susceptible to timing and power analysis

LWC Initiatives and Standards - CAESAR (2014-2018)

Goal: To select a portfolio of algorithms with advantages over AES-GCM, and suitable for widespread adoption for

- **Constrained environments:** fits into small hardware area, small code for 8-bit CPUs, side channel resistance, hardware performance, especially energy/bit, speed on 8-bit CPUs, optimized for short messages,
- High performance applications, and defense in depth.

Received 57 submissions in March'14, finalists announced in March'18.

Finalists for constrained environments:

- Ascon: 320-bit permutation using the MonkeyDuplex mode.
- ACORN: Stream cipher based using LFSRs

LWC Initiatives and Standards - CRYPTREC

Goal: To evaluate and monitor the security of cryptographic techniques used in Japanese e-Government systems.

Publishes three lists:

- e-Government recommended ciphers list
- Candidate recommended ciphers list
- Monitored ciphers list

In March'17, published a guideline on lightweight cryptography with target algorithms:

- Block ciphers: AES, Camellia, CLEFIA, TDES, LED, PRINCE, PRESENT, Piccolo, TWINE, SIMON, SPECK, Midori.
- Authenticated Encryption: ACORN, AES-GCM, AES-OTR, Ascon, CLOC, SILC, JAMBU, Ketje, Minalpher, AES-OCB.

ISO/IEC

ISO/IEC JTC 1/SC 27 focus on IT Security techniques

- A standardization subcommittee of International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Five working groups
  - Working Group 2 (WG2) is for Cryptography and Security Mechanisms. Lightweight Crypto is one of the projects of WG2. The standards developed under this project are in ISO/IEC 29192 series.

ISO/IEC 29192 Lightweight Cryptography (1/3)

Part 1 - General (2012)

- Defines security, classification and implementation requirements.
- 80-bit security is considered as minimum security strength for lightweight cryptography. At least 112-bit security is recommended for longer periods.

Part 2 - Block ciphers

- PRESENT: block size of 64 bits, key size of 80 or 128 bits (CHES 2007)
- CLEFIA: block size of 128 bits, key size of 128, 192, 256 bits (FSE 2007)
- Amendment 1 was proposed to include SIMON and SPECK, but it was not approved.
- Amendment 2 specifies a Korea algorithm LEA (final stage of publications)

ISO/IEC 29192 Lightweight Cryptography (2/3)

Part 3 - Stream ciphers

- Enocoro: key size of 80 or 128 bits, based on a finite state machine and uses operations defined over the finite field $GF(2^4)$ and $GF(2^8)$.
- Trivium: key size of 80 bits, three nonlinear feedback registers, 288 bits of internal size.

Part 4 - Asymmetric techniques

- An unilateral authentication mechanism based on discrete logarithms on elliptic curves;
- An authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key;
- An identity-based signature mechanism.

ISO/IEC 29192 Lightweight Cryptography (3/3)

Part 5 - Hash functions

- Photon with permutation sizes 100, 144, 196, 256 and 288 bits and hash sizes 80, 128, 160, 224 and 256 respectively.
- Spongent with permutation sizes of 88, 136, 176, 240 and 272 bits and hash sizes 88, 128, 160, 224, and 256 respectively
- Lesamnta-LW with permutation size 384 bits and hash size 256 bits

Part 6 - MAC

- Includes three algorithms : LightMAC, Tsudik's keymode, Chaskey-12.

Part 7 - Broadcast Authentication Protocols

- Specifies Timed Efficient Stream Loss-Tolerant Authentication

Part 8 - Authenticated Encryption

- First working draft, specifying Grain-128A

ISO/IEC 29167 Automatic identification and data capture techniques

- Part I -Security services for RFID air interfaces: Defines various security mechanisms that can be implemented by a tag, and the requirements for crypto suites.
- Part 10-21 includes AES-128, Present-80, ECC-DH, Grain-128A, AES OFB, XOR, ECDSA-ECDH, cryptoGPS, RAMON, SPECK, SIMON.

NIST Lightweight Cryptography Standardization Process

AES in Constrained Environments

- Many optimized implementations of AES in hardware and software
  - Encryption only, ultra small area 1457 gates (Shreedhar et al., 2019)
  - Sub-atomic AES implementation of enc/dec + key schedule (Wamser et al., 2017)
  - Atomic-AES implementation of enc/dec core (Banik et al., 2016)
  - 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015)
  - Fast AES-128-CTR on ARM Cortex-M3 with side channel resistance (Schwabe, Stoffelen, 2016)

AES in Constrained Environments

- Many optimized implementations of AES in hardware and software
  - Encryption only, ultra small area 1457 gates (Shreedhar et al., 2019)
  - Sub-atomic AES implementation of enc/dec + key schedule (Wamser et al., 2017)
  - Atomic-AES implementation of enc/dec core (Banik et al., 2016)
  - 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015)
  - Fast AES-128-CTR on ARM Cortex-M3 with side channel resistance (Schwabe, Stoffelen, 2016)
- Not always feasible to implement, e.g., on RL78 16-bit microcontroller, combined enc/dec implementation is not possible within 512 bytes of ROM and 128 bytes of RAM (Moriai, 2016).

AES in Constrained Environments

- Many optimized implementations of AES in hardware and software
  - Encryption only, ultra small area 1457 gates (Shreedhar et al., 2019)
  - Sub-atomic AES implementation of enc/dec + key schedule (Wamser et al., 2017)
  - Atomic-AES implementation of enc/dec core (Banik et al., 2016)
  - 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015)
  - Fast AES-128-CTR on ARM Cortex-M3 with side channel resistance (Schwabe, Stoffelen, 2016)
- Not always feasible to implement, e.g., on RL78 16-bit microcontroller, combined enc/dec implementation is not possible within 512 bytes of ROM and 128 bytes of RAM (Moriai, 2016).
- AES is fast on 8-bit microcontrollers, but requires to store the Sbox.

AES in Constrained Environments

- Many optimized implementations of AES in hardware and software
  - Encryption only, ultra small area 1457 gates (Shreedhar et al., 2019)
  - Sub-atomic AES implementation of enc/dec + key schedule (Wamser et al., 2017)
  - Atomic-AES implementation of enc/dec core (Banik et al., 2016)
  - 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015)
  - Fast AES-128-CTR on ARM Cortex-M3 with side channel resistance (Schwabe, Stoffelen, 2016)
- Not always feasible to implement, e.g., on RL78 16-bit microcontroller, combined enc/dec implementation is not possible within 512 bytes of ROM and 128 bytes of RAM (Moriai, 2016).
- AES is fast on 8-bit microcontrollers, but requires to store the Sbox.
- Devices with hardware acceleration modules may have side channel vulnerabilities. e.g., updates for Phillips light bulbs are authenticated using AES-based MAC with fixed (secret) key, possible to recover key and push malicious updates (Ronen et al, 2017)

SHA-2 and SHA-3 Families in Constrained Environments

- Large memory requirements, 1600 bits for SHA-3 and 512 bits for SHA-2.
- Lightweight versions of SHA-3 with smaller permutation sizes (200-, 400- and 800-bits) are specified in the FIPS 202, but currently not approved.

Do we need lightweight cryptography standards?

- Dedicated algorithms with inherent side channel resistance may provide security and performance advantages over AES.
- Hash functions with smaller internal size, and that can share crypto logic to provide other functionalities are more suitable for constrained devices.

NIST LWC Project

Goal: Developing new guidelines, recommendations and standards for constrained environments when the performance of the current NIST standards is not acceptable.

- Not a 'drop-in-replacement' for the current standards, rather an addition to the portfolio of NIST standards.

NIST LWC Project

Goal: Developing new guidelines, recommendations and standards for constrained environments when the performance of the current NIST standards is not acceptable.

- Not a 'drop-in-replacement' for the current standards, rather an addition to the portfolio of NIST standards.

Scope: Symmetric-key cryptography: Authenticated Encryption with Associated Data (AEAD) with optional hashing functionality.

NIST LWC Project

Goal: Developing new guidelines, recommendations and standards for constrained environments when the performance of the current NIST standards is not acceptable.

- Not a 'drop-in-replacement' for the current standards, rather an addition to the portfolio of NIST standards.

Scope: Symmetric-key cryptography: Authenticated Encryption with Associated Data (AEAD) with optional hashing functionality.

Standardization process:

- Multi-year competition-like process similar to PQC, AES, SHA3, CAESAR.
- Supported by workshops, open discussions via emailing forum.
- Benefit from the knowledge and insights from CAESAR and SHA3 competitions.

So far ...

Date	Event
July, 2015	First Lightweight Cryptography Workshop
October, 2016	Second Lightweight Cryptography Workshop at NIST
March, 2017	NISTIR 8114 Report on Lightweight Cryptography
April, 2017	(Draft) Profiles for LWC Standardization Process
May, 2018	Federal Register Notice for submission requirements
August, 2018	Federal Register Notice for the call
February, 2019	Submission deadline
March, 2019	Amendment deadline
April, 2019	Announcement of the Round 1 Candidates
August, 2019	Announcement of the Round 2 Candidates
October, 2019	NISTIR 8268 Status Report on the First Round
November, 2019	Third Lightweight Cryptography Workshop

Submission Requirements

- Publicly disclosed and freely available during the process with signed IP statements that disclose patent info
- Requirements on functionality: AEAD, and the (optional) hash function
- Requirements on the security, and theoretical and empirical evidence providing justification for security claims
- Requirements on the design goals and implementations

AEAD Security Requirements

- Confidentiality of the plaintexts (under adaptive chosen-plaintext attacks) + Integrity of the ciphertexts (under adaptive forgery attempts)
- Well-understood and analyzed designs.
- At least 128-bit keys, attacks requiring at least 2^{112} computations (nonce is assumed to be unique under the same key.)
- Family of (at most 10) algorithms
  - 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 Function Security Requirements

- 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 should lend themselves to countermeasures against side channel attacks, and fault attacks.
- Reference implementations to support understanding of the design.
- Compatible API with eBACS: ECRYPT Benchmarking of cryptographic systems.

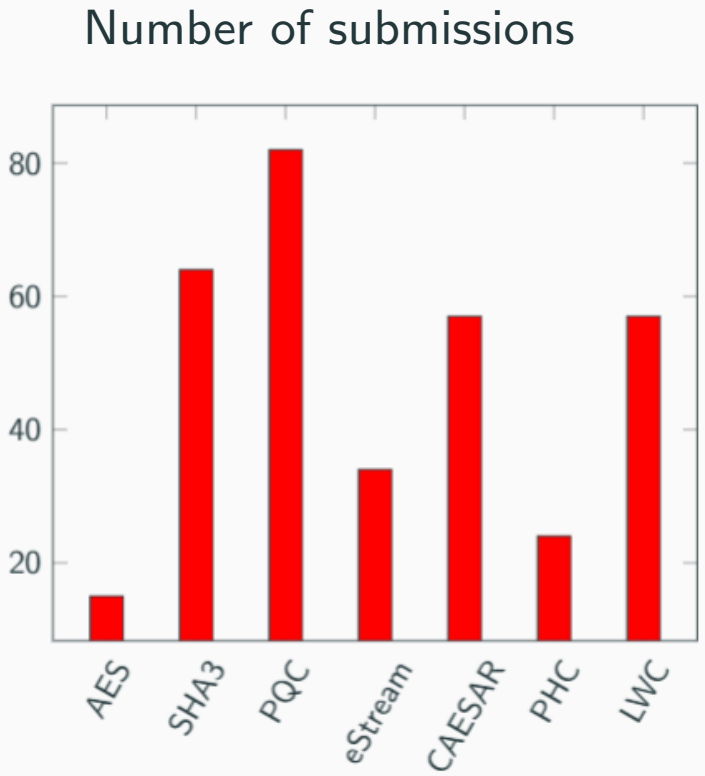
The Submissions

Early Review Process - Jan. 4, 2019

- 8 early submissions
- Sent suggestions and feedback to increase the quality of the submissions

Submission Deadline - Feb. 25, 2019

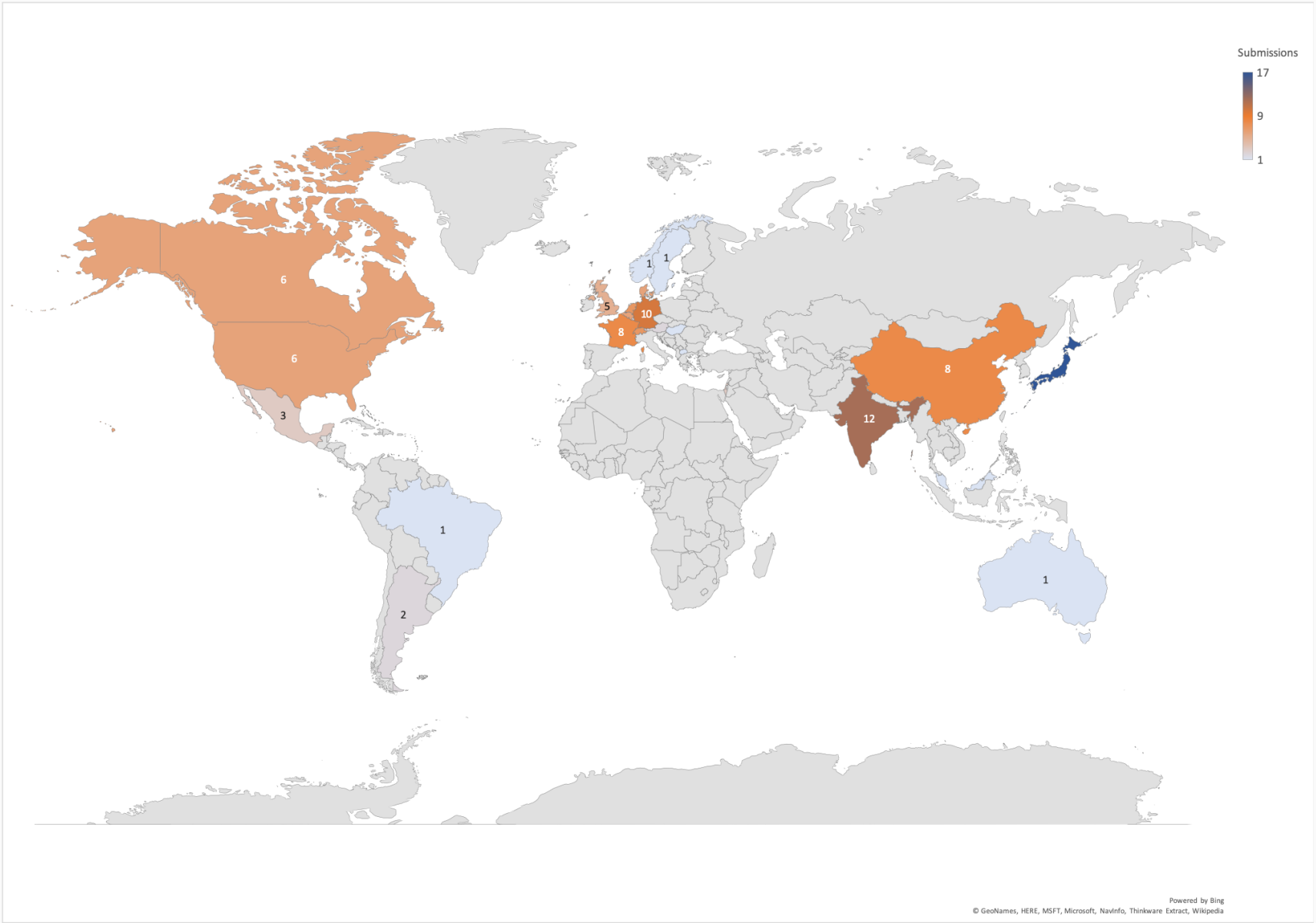
- 57 submissions (129 submitters).
- One additional month to amend submissions to reduce the effects of the 35-day U.S. Government shutdown.



Round 1 Candidates

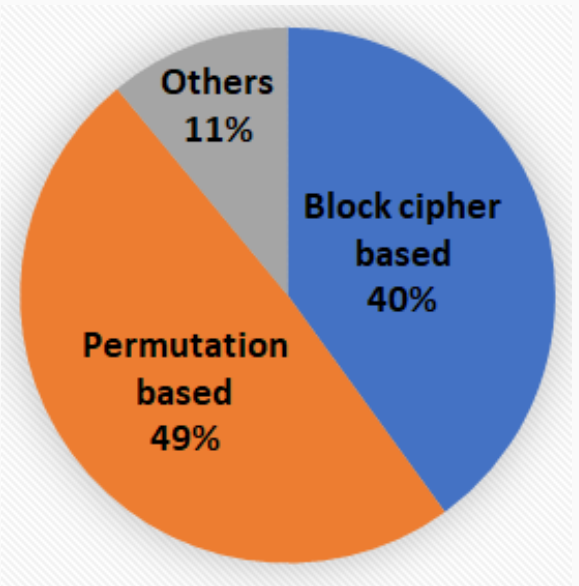
After a month of internal preliminary analysis, NIST announced **56** Round 1 Candidates in April, 2019.

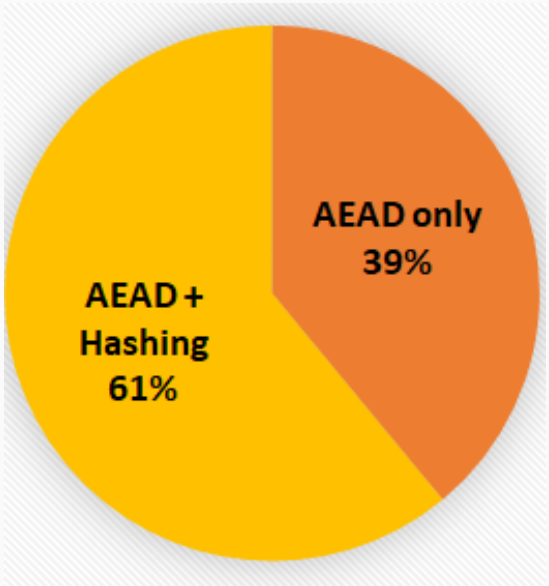
Where Did Submissions Come From?



Design Approaches

- Permutation-based designs
  - Typically support both AEAD and hashing
  - Small permutations (250-400 bits)
- (Tweakable) block cipher designs
  - Typically just support AEAD functionality
- Stream cipher based designs and others





Common Issues with the Round 1 Candidates

- Practical forgery attacks due to domain separation problems
- Practical forgery attacks due to padding problems
- Practical distinguishers, and undesirable properties
- Not handling empty message or associated data
- Implementation errors, inconsistencies between specification and reference implementation
- New designs with no third party analysis

Attacks & Observations	***Candidates***
Forgery attacks	Bleep64, CLAE, FlexAEAD, GAGE and InGAGE , HERN and HERON, Liliput-AE, Limdolen, Qameleon, Quartet, Remus, Simple, SIV-Rijndael256, SIV-TEM-PHOTON, SNEIK, Sycon, TGIF, Triad
Length-extension attacks	CiliPadi, FlexAEAD
Distinguishing attacks	Limdolen
Undesirable properties	LAEM, SNEIK, TRIFLE, CLX

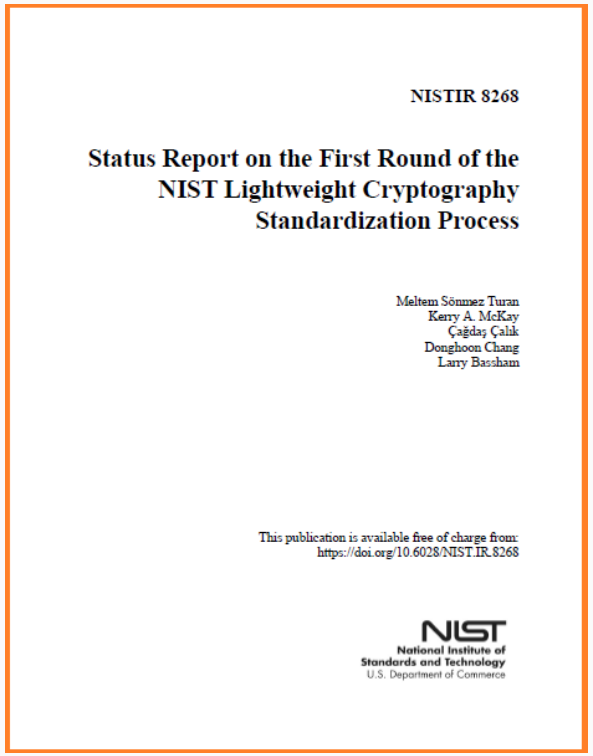
End of Round 1

NIST shortened the duration of the Round 1 from 12 months to 4 months to focus the analysis on the more promising candidates.

Selection criteria for Round 2:

- Cryptographic security of the candidates
- Maturity of the candidates
- (Performance was not considered)

In October 2019, NIST published NISTIR 8268 - Status Report on the First Round.


NISTIR 8268

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

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalik
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

Round 2 Candidates

- In August 2019, NIST selected 32 Round 2 candidates.

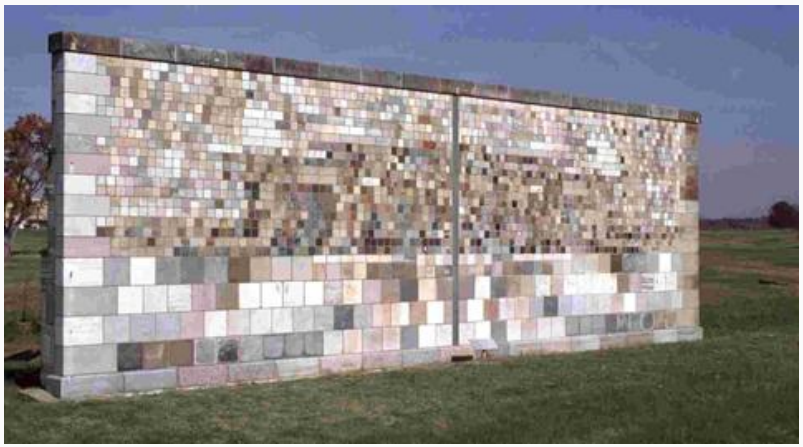
ACE	ASCON	COMET
DryGASCON	Elephant	ESTATE
ForkAE	GIFT-COFB	Gimli
Grain-128AEAD	HyENA	ISAP
KNOT	LOTUS-AEAD & LOCUS-AEAD	mixFeed
ORANGE	Oribatida	PHOTON-Beetle
Pyjamask	Romulus	SAEAES
Saturnin	SKINNY-AEAD & -HASH	SPARKLE
SPIX	SpoC	Spook
Subterranean 2.0	SUNDAE-GIFT	TinyJAMBU
WAGE	Xoodyak	

- Submitters were allowed to update their packages to correct typos, fix bugs, and to include additional content (such as optimized implementations or new security analysis).
- Design tweaks were not allowed.

Evaluation of Round 2 Candidates

Resources

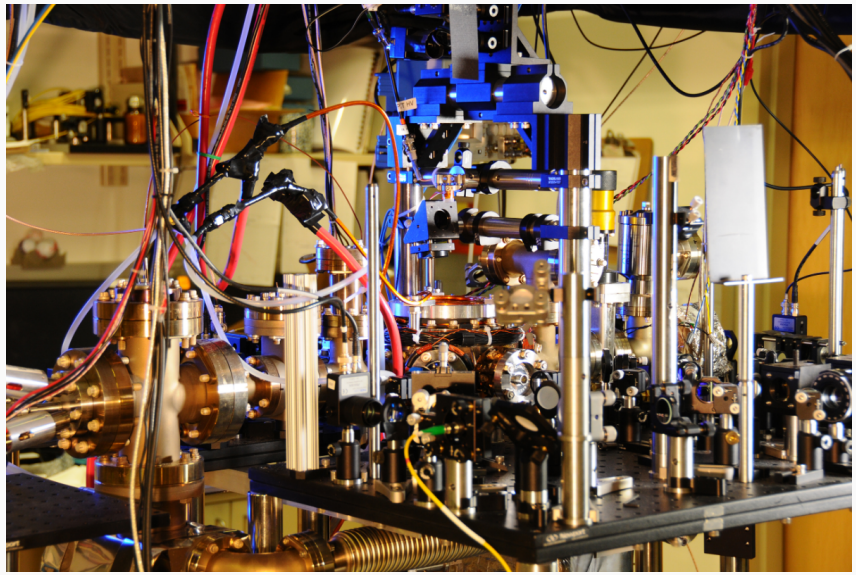
- Internal and external cryptanalysis
- Workshops
- Official comments (can be submitted on lwc-forum or our website)
- Research publications
- Hardware and software performance benchmarks



📷: NIST Stone Wall (constructed to study the performance of stone subjected to weathering.)

Next Steps and Tentative Timeline

- Analysis and comparison of round 2 candidates for about a year
- Select around eight candidates (finalists) to advance to Round 3 in September 2020 (tentative timeline)
- Organize the fourth LWC workshop
- Select winner(s) in 2021



NIST Atomic clock by Burrus/NIST

Thanks!

Project webpage:
`https://www.nist.gov/programs-projects/lightweight-cryptography`

Forum: `lwc-forum@list.nist.gov` (500+ members)

Contact email: `lightweight-crypto@nist.gov`

#NISTLWC

Announcements - Digital Signatures

FIPS 186-5 and SP 800-186 drafts are published in October 2019.

- DSA no longer approved for signature generation.
- X9.31 RSA signatures removed.
- Larger key sizes (3072 bits or more) for RSA signatures allowed.
- New elliptic curves specified (Edwards25519 and Edwards448).
- The EdDSA signature algorithm is included.
- Deterministic version of ECDSA included.
- Various minor improvements/corrections to algorithms in appendices.

Send your comments to **fips186-comments@nist.gov** by **January 29, 2010**.