NIST's Lightweight Crypto Standardization Process

Meltem Sönmez Turan

CRYPTREC Symposium

December 18, 2017 Tokyo, Japan

National Institute of Standards and Technology

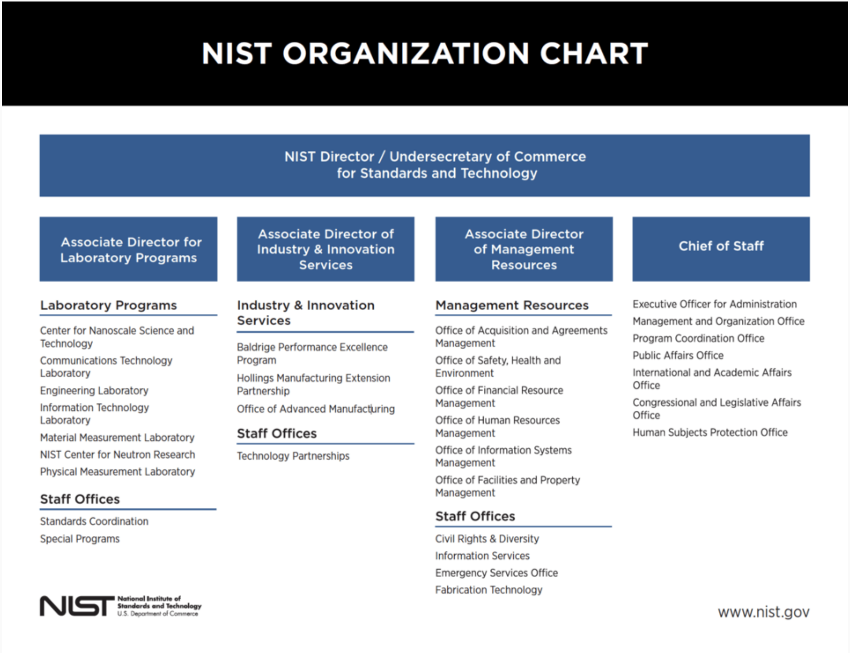
- Non-regulatory federal agency within U.S. Department of Commerce.
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988.
- Headquarters in Gaithersburg, Maryland, and laboratories in Boulder, Colorado.
- Employs around 3,000 employees, and 2700 associates.

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 3,000 employees, and 2700 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

NIST Director / Undersecretary of Commerce for Standards and Technology

Associate Director for Laboratory Programs

Laboratory Programs

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

Staff Offices

- Standards Coordination
- Special Programs

Associate Director of Industry & Innovation Services

Industry & Innovation Services

- Baldrige Performance Excellence Program
- Hollings Manufacturing Extension Partnership
- Office of Advanced Manufacturing

Staff Offices

- Technology Partnerships

Associate Director of Management Resources

Management Resources

- Office of Acquisition and Agreements Management
- Office of Safety, Health and Environment
- Office of Financial Resource Management
- Office of Human Resources Management
- Office of Information Systems Management
- Office of Facilities and Property Management

Staff Offices

- Civil Rights & Diversity
- Information Services
- Emergency Services Office
- Fabrication Technology

Chief of Staff

- Executive Officer for Administration
- Management and Organization Office
- Program Coordination Office
- Public Affairs Office
- International and Academic Affairs Office
- Congressional and Legislative Affairs Office
- Human Subjects Protection Office

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

www.nist.gov

Computer Security Division (CSD)

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

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

What does CSD do?

- **Algorithm Specification:** Federal Information Processing Standards (FIPS) and Special Publications (SP) specify a number of approved cryptographic algorithms.
- **General guidance on the use of cryptography:** Covering selection, implementation, deployment and use of cryptography.
- **Guidelines in application specific areas:** Areas of particular need for the US government (e.g., PIV, TLS)
- **Testing:** Providing assurance that crypto is implemented properly (e.g., FIPS 140 and CMVP).

Who does CSD work with?

- **Government:** Core user community.
- **Industry:** On adoption of cryptographic algorithms, feedback mechanism on standards.
- **Academic Researchers:** Development of new algorithms/modes/ schemes to advance science of cryptography.
- **Standards Developing Organizations:** Adoption and development of new standards.

How does CSD develop standards?

- **International competitions:** Engage community through an open competition (e.g., AES, SHA-3).
- **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).

NIST's Lightweight Crypto Project

Motivation

- Shift from general-purpose computers to dedicated resource-constrained devices.
- New applications (e.g., cyber physical systems, IoT).
- Lack of crypto standards that are suitable for constrained devices.

Goal

- Understanding the need for lightweight crypto.
- Developing new lightweight crypto standards.

So far ...

The project started in 2014.

Two workshops:

- First Lightweight Crypto Workshop at NIST, July 2015.
- Second Lightweight Crypto Workshop at NIST, October 2016.

So far ...

The project started in 2014.

Two workshops:

- First Lightweight Crypto Workshop at NIST, July 2015.
- Second Lightweight Crypto Workshop at NIST, October 2016.

Consensus that there is need for lightweight crypto standards.

NISTIR 8114 - Report on Lightweight Cryptography

The report was published in March 2017 (after 90-day comment period).

Report provides information on:

- Overview of lightweight cryptography: Target devices, performance metrics, lightweight primitives, performance of NIST standards in constrained environments, and other lightweight crypto standards.
- NIST's Lightweight Crypto Project: Scope, design considerations, profiles, and evaluation process.

What is Lightweight Cryptography?

- Subfield of cryptography that aims to provide crypto solutions tailored to constrained environments.
- Lightweight cryptography does not mean weak crypto.
- Security properties may be different than those desired for general use, but must be sufficient for the target application.
- Lightweight crypto may
  - be less robust,
  - be less misuse resistant,
  - have fewer features.

Target Devices

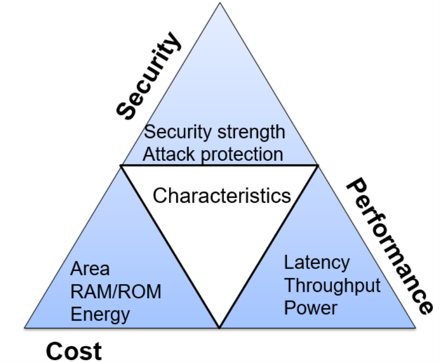
Wide variety of devices on broad spectrum of hardware and software

- Conventional cryptography for servers, desktops, smart phones, tablets, etc.
- Lightweight cryptography for embedded systems, sensor networks, RFID tags, etc.

Tradeoff between Security, Performance and Cost

Optimal tradeoff depends on the target technology and application!

- For hardware applications: Area, latency, throughput, power/energy consumption etc.
- For software applications: Execution time, latency, memory (ROM/RAM) requirements, power/energy consumption.



Due to the variability of applications/requirements, hard to select a one-size-fits-all algorithm!

New Lightweight Designs

Design strategies:

- Many iterations of simple rounds, simple operations (e.g., XORs, rotation, 4x4 Sboxes, bit permutations).
- Smaller block/key sizes, smaller security margins by design.
- Simpler key schedules.

Modifications of well-analyzed designs: e.g., DESL, DESXL.

Old interesting algorithms: e.g., RC5, TEA, XTEA.

New dedicated algorithms: e.g., GIMLI, Skinny, Pride, Simon, Speck, Simeck, Present, etc.

NIST Standards in Constrained Environments

AES

- 1947/2090 GEs (8-bit serial implementation) (Mathew et al., 2015).
- 2400 GEs (Moradi et al., 2011).
- 8-bit AVR microcontrollers 124.6 and 181.3 cpb for enc/dec with a code size <2Kbyte.
- On RL78 16-bit microcontroller, combined enc/dec implementation is not possible within 512 bytes of ROM and 128 bytes of RAM (Moriai, 2016).

SHA-3

- Area requirement is around 5500GEs, with low but acceptable throughput.

Conventional cryptography algorithms should be used whenever the performance is acceptable!

Lightweight Cryptography Standards (1/2)

ISO/IEC 29192 Lightweight Cryptography

- Block ciphers: PRESENT and CLEFIA
- Stream ciphers: Enocoro and Trivium
- Asymmetric techniques: cryptoGPS, authentication and key exchange mechanism ALIKE, and ID-based signature IBS
- Hash functions: Photon, Spongent and Lesamnta-LW
- MAC: under development

ISO/IEC 29167

- Dedicated to RFID communications, and includes AES-128, Present-80, ECC-DH, Grain-128A, AES OFB, ECDSA-ECDH, cryptoGPS and RAMON

Lightweight Cryptography Standards (2/2)

ECRYPT eSTREAM Project

- a 4-year network of excellence funded project started in 2004 by European Network of Excellence for Cryptology (ECRYPT)
- Profile II : for hardware applications with restricted resources with key size of 80 bits. Finalists: Grain, Trivium, Mickey

Industry-Specific Standards

- Proprietary designs
- Examples: A5/1 (in GSM), E0 (in Bluetooth), Crypto1 (in Mifare RFID tags), Cryptomeria (C2) (for digital rights managements), Dect (cordless phones), DST40 (TI), KeeLoq (authentication in car locks), Kindle stream cipher
- Most reverse-engineered, and practically broken.

NIST's Lightweight Crypto Project

Scope:

- All cryptographic primitives and modes that are needed in constrained environments.
- Initial Focus: Symmetric Crypto

Standardization Plan:

- Develop and maintain a portfolio of lightweight algorithms and modes that are approved for limited use.
- The lightweight portfolio is not intended to offer alternative algorithms for general use.
- Algorithm properties will be summarized by *profiles*.

Profiles

The profiles are intended to specify requirements for lightweight algorithms that:

- satisfy performance requirements on specific platforms that are not met by current NIST standards;
- offer significant implementation or performance improvements compared to the current NIST standards on specific platforms; and
- provide security against cryptanalysis, even in the presence of side-channel information.

Profile Template

Profile<profile name>	
Functionality	Purpose of cryptographic algorithm (e.g., encryption, authenticated encryption scheme, hashing, message authentication, etc.)
Design goals	List design goals.
Physical characteristics	Name physical characteristic(s), and provide acceptable range(s) (e.g., 64 to 128 bytes of RAM)
Performance characteristics	Name performance characteristic(s), and provide acceptable range(s) (e.g., latency of no more than 5 ns)
Security characteristics	Minimum security strength, relevant attack models, side channel resistance requirements, etc.

Developing Profiles

NISTIR 8114 included 22 questions to industry partners to understand their lightweight crypto need.

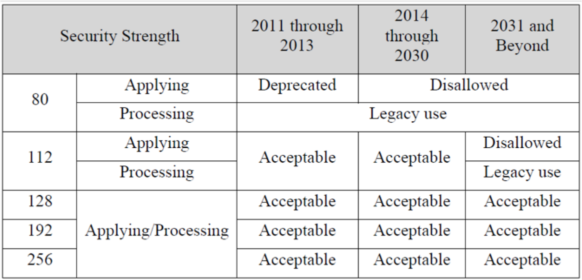
- Application: Target functionality? Typical plaintext, tag sizes?
- Constraints: What limits are imposed on the energy and/or power that is available to the device? Does the device have to respond within a specific time?
- Cryptographic keys: How are keys generated? Where are they stored, and for how long? How much data is processed under the same key?
- Software implementations: Which platforms? Which specific types of processors? Limits on the amount of registers, RAM and ROM? Is it necessary to obfuscate the implementation?
- Hardware implementations: Which types of hardware are considered (FPGA, ASIC, etc.)? Limits on the amount of logic blocks or GEs?
- Side channel resistance: Side-channel or fault attacks required?

Responses to the Questionnaire

- Target applications: Hardware encrypted data storage device, low-cost and low-consumption sensor data transmission, RAIN RFID tags for anti-counterfeiting solutions, IoTs, wearables, low power wireless sensor networks.
- Target functionality: Encryption, AE, hashing, key agreement, sensor/tag authentication, with plaintext size of 16 bytes
- Target devices: ARM Cortex-M0 processors, Intel Quark SoC X1021, Atom E3826
- Side channel resistance: In general, good to have.

Discussion Points - Key sizes

Many designs made tradeoff of using smaller key sizes to reduce cost.
NIST SP 800 131A makes recommendations about security strengths.



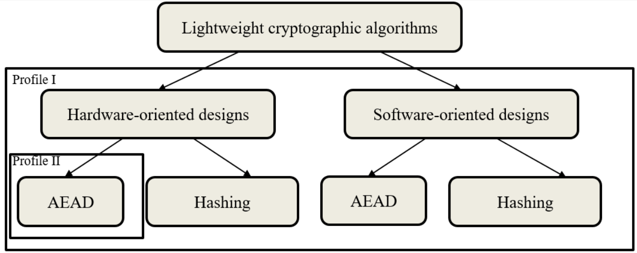
Security Strength		2011 through 2013	2014 through 2030	2031 and Beyond
80	Applying	Deprecated	Disallowed	
	Processing	Legacy use		
112	Applying	Acceptable	Acceptable	Disallowed
	Processing			Legacy use
128	Applying/Processing	Acceptable	Acceptable	Acceptable
192		Acceptable	Acceptable	Acceptable
256		Acceptable	Acceptable	Acceptable

Key sizes of at least 128 bits, and security level of at least 112 bits.

Draft Profiles for Lightweight Cryptography

NIST published Draft White Paper *Profiles for Lightweight Cryptography Standardization Process* in April 2017.

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


Lightweight cryptographic algorithms
Profile I
Hardware-oriented designs
Software-oriented designs
Profile II
AEAD
Hashing
AEAD
Hashing

Profile I - AEAD and Hashing for Constrained Environments (1/4)

Functionality:

- Authenticated encryption with associated data and hashing

Design goals:

- Performs significantly better in constrained environments (hardware and embedded software platforms) compared to current NIST standards.
- Both algorithms should be optimized to be efficient for short messages (e.g., as short as 8 bytes).
- The message length shall be an integer number of bytes.

Physical characteristics

- Compact hardware implementations and embedded software implementations with low RAM and ROM usage should be possible.

Profile I - AEAD and Hashing for Constrained Environments (2/4)

Performance characteristics:

- The performance on ASIC and FPGA should consider various standard cell libraries, the flexibility to support various implementation strategies (low energy, low power, low latency), with significant improvements over current NIST standards.
- The performance on microcontrollers should consider a wide range of 8-bit, 16-bit and 32-bit microcontroller architectures.
- The preprocessing of a key (in terms of computation time and memory footprint) should be efficient.

Profile I - AEAD and Hashing for Constrained Environments (3/4)

Security characteristics for AEAD

- A key length of 128 bits shall be supported.
- Nonce and tag lengths of up to 128 bits shall be supported.
- Plaintext and associated data lengths of up to $2^{50} - 1$ bytes shall be supported.
- At least $2^{50} - 1$ bytes can be processed securely under a single key.
- Cryptanalytic attacks should require at least 2^{112} computations on a classical computer in a single-key setting.
- Lends itself to countermeasures against various side-channel attacks, including timing attacks, simple and differential power analysis (SPA/DPA), and simple and differential electromagnetic analysis (SEMA/DEMA).

Profile I - AEAD and Hashing for Constrained Environments (4/4)

Security characteristics for hashing

- Cryptanalytic attacks should require at least 2^{112} computations on a classical computer.
- Hash outputs of 256 bits must be supported, and longer hash values may be supported as well.
- A maximum message length of $2^{50} - 1$ bytes shall be supported.
- Lends itself to countermeasures against various side-channel attacks, including timing attacks, simple and differential power analysis (SPA/DPA), and simple and differential electromagnetic analysis (SEMA/DEMA).

Profile II- AEAD for Constrained Hardware Environments (1/2)

Functionality:

- Authenticated encryption with associated data

Design goals:

- Performs significantly better compared to current NIST standards.
- The performance for short messages (e.g., as short as 8 bytes) is important.
- The message length shall be an integer number of bytes.

Physical characteristics

- Targeted towards constrained hardware platforms.
- Compact hardware implementations should be possible.

Profile II - AEAD for Constrained Hardware Environments (2/2)

Performance characteristics:

- The performance on ASIC and FPGA should consider a wide range of standard cell libraries and vendors.
- Algorithm should be flexible to support various implementation strategies (low energy, low power, low latency).
- The preprocessing of a key (in terms of computation time and memory footprint) should be efficient.

Security characteristics:

- Same as security characteristics of AEAD in Profile I.

Current Status

- Developing the submission, evaluation, and selection processes (e.g., submission requirements, API, evaluation methods).
- Preparing a single call for submissions for both profiles: AEAD with optional hashing.

Next Steps

- NIST will publish a draft call for submission of lightweight cryptographic functions.
- NIST will finalize the call for submission.
- NIST will organize Lightweight Cryptography Workshops to discuss the performance and security properties of submissions, and plans for standardization.

Thanks!

More information available at

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

Subscribe to our mailing list: `lwc-forum@list.nist.gov`

Additional comments/questions?

Email the team at `lightweight-crypto@nist.gov`