Standards of Cryptographic Algorithms at NIST

Cryptographic Technology Group, Computer Security Division

Information Technology Laboratory, National Institute of Standards and Technology

Cryptography Standards at NIST

The development of cryptography standards fits the NIST 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.

Within NIST, the standards for cryptographic algorithms are developed within the Computer Security Division. Several groups collaborate in the area of cryptography, e.g., to develop algorithms and validate their implementation.

- **Information Technology Laboratory (ITL):** advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.
- **Computer Security Division (CSD):** Cryptographic Technology; Secure Systems and Applications; Security Components and Mechanisms; Security Engineering and Risk Management; Security Testing, Validation and Measurement.
- **Cryptographic Technology Group (CTG):** research, develop, engineer, and produce guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols.

Main types of Publications

FIPS — **F**ederal **I**nformation **P**rocessing **S**tandard

SP 800 — **S**pecial **P**ublication in Computer Security

NISTIR — **NIST** **I**nternal or **I**nteragency **R**eport

ITLB — **I**nformation **T**echnology **L**aboratoty **B**ulletin

- **FIPS:** Standards and guidelines for federal computer systems developed in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce. `https://www.nist.gov/itl/fips-general-information`
- **SP 800:** Presents information of interest to the computer security community. The series comprises guidelines, recommendations, technical specifications, and annual reports of NISTs cybersecurity activities. `https://csrc.nist.gov/publications/sp800`
- **NISTIR:** Reports of research findings, including background information for FIPS and SPs. `https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir`
- **ITL Bulletin:** Monthly overviews of NIST's security and privacy publications, programs and projects. `https://csrc.nist.gov/publications/itl-bulletin`

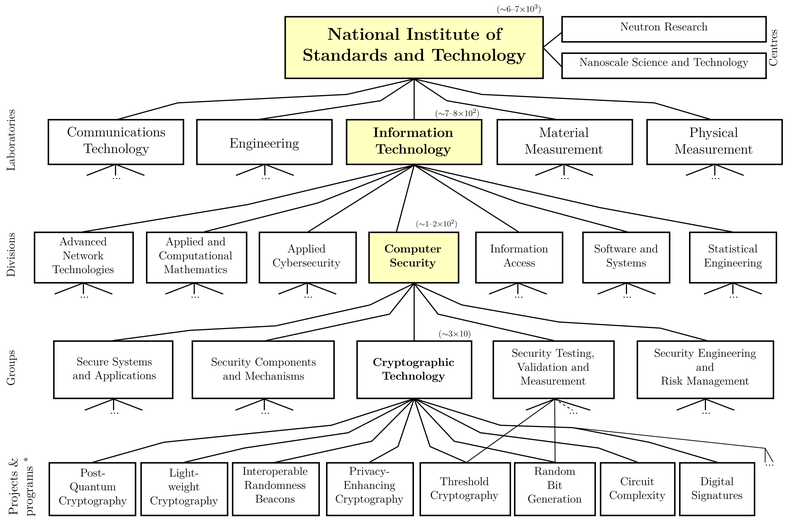
Examples of ongoing activities

The Crypto group develops new **standards**, and also develops **applications** and performs **research** that promote adoption of better cryptographic technologies. Examples:

- New standards for **Post-Quantum Cryptography (PQC)**
- New standards for **Lightweight Cryptography project (LWC)**
- New standards for **Threshold Cryptography (TC)**
- Reference material in **Privacy Enhancing Cryptography (PEC)**
- Applications for **Interoperable Randomness Beacons**
- Research on **Circuit complexity**
- Revised standards for **Digital Signatures**
- New and revised methods for **Random Bit Generation**
- New and revised guidance on **Key management**

Find more detailed info at `https://www.nist.gov/itl/csd/cryptographic-technology`

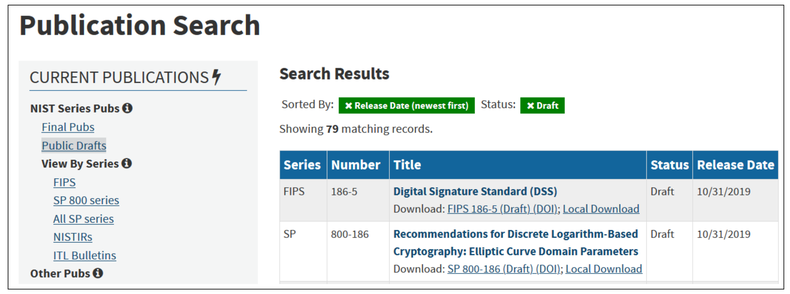
Computer security and cryptography at NIST



* (Some projects/programs involve several groups, divisions or labs) (in parenthesis: approximate range # workers, inc. associates and fed. employees)

Computer Security Resource Center (CSRC)

The Computer Security Division maintains a Computer Security Resource Center (CSRC), with documentation on publications, projects, news, and events.



Screenshots from: `https://csrc.nist.gov/publications/draft-pubs`

The test of time

Which of today's developing standards will remain, 70 years from now, as building blocks of advanced cryptography?

The NIST Stone Test Wall: "Constructed [in 1948] to study the performance of stone subjected to weathering. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 states, and 320 are stones from 16 foreign countries."

Photo in 2018: `https://www.nist.gov/sites/default/files/documents/2018/06/15/nist_gaithersburg_master_plan_may_7_2018.pdf`

Photo in 1948: `https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall`

Examples of relevant publications

The following lists are not exhaustive

FIPS:

- FIPS 180: Secure Hash Standard (SHS)
- FIPS 186: Digital Signature Standard (DSS)
- FIPS 197: Advanced Encryption Standard (AES)
- FIPS 198: The Keyed-Hash Message Authentication Code (HMAC)
- FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

SP 800:

(R. denotes "Recommendation for")

- **SP 800-22:** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- **SP 800-32:** Introduction to Public Key Technology and the Federal PKI Infrastructure.
- **SP 800-38:** R. Block Cipher Modes of Operation (it is a series of publications A–G)
- **SP 800-52:** Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- **SP 800-56:** R. Pair-Wise Key-Establishment Schemes Using: Discrete Logarithm Cryptography (SP 800-56A); and Integer Factorization Cryptography (SP 800-56B).
- **SP 800-56C:** R. Key-Derivation Methods in Key-Establishment Schemes.
- **SP 800-57:** R. for Key Management
- **SP 800-90A:** R. Random Number Generation Using Deterministic Random Bit Generators
- **SP 800-90B:** R. Entropy Sources Used for Random Bit Generation
- **SP 800-90C:** R. Random Bit Generator (RBG) Constructions
- **SP 800-108:** Recommendation for Key Derivation Using Pseudorandom Functions
- **SP 800-132:** R. Password-Based Key Derivation
- **SP 800-133:** R. Cryptographic Key Generation
- **SP 800-185:** SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash
- **SP 800-186:** R. Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters

Guidance on cryptography standards:

There are also guidelines on how to develop, implement and use other crypto standards.

- **NISTIR 7977:** Cryptographic Standards and Guidelines Development Process
- **SP 800-175:** Guideline for Using Cryptographic Standards in the Federal Government
- **FIPS 140:** Security Requirements for Cryptographic Modules.

The development of several standards benefits from the collaboration of several groups.

Poster produced for: NIST-ITL Science Day 2019 — November 06, 2019 (Gaithersburg, USA)

Poster presented by: Luís T. A. N. Brandão, Elaine Barker, René Peralta