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

NIST Standards for Cryptographic Algorithms

Cryptographic Technology Group, Computer Security Division

Information Technology Laboratory, National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Cryptography Standards at NIST

Crypto standards fit in the NIST mission: innovation, competitiveness, standards and technology, economic security and quality of life.

Crypto algorithms are developed and analyzed in the Computer Security Division (CSD). Several groups collaborate (develop, validate, ...).

Main types of Publications

FIPS
Federal Information Processing Standard

SP 800
Special Publication in Computer Security

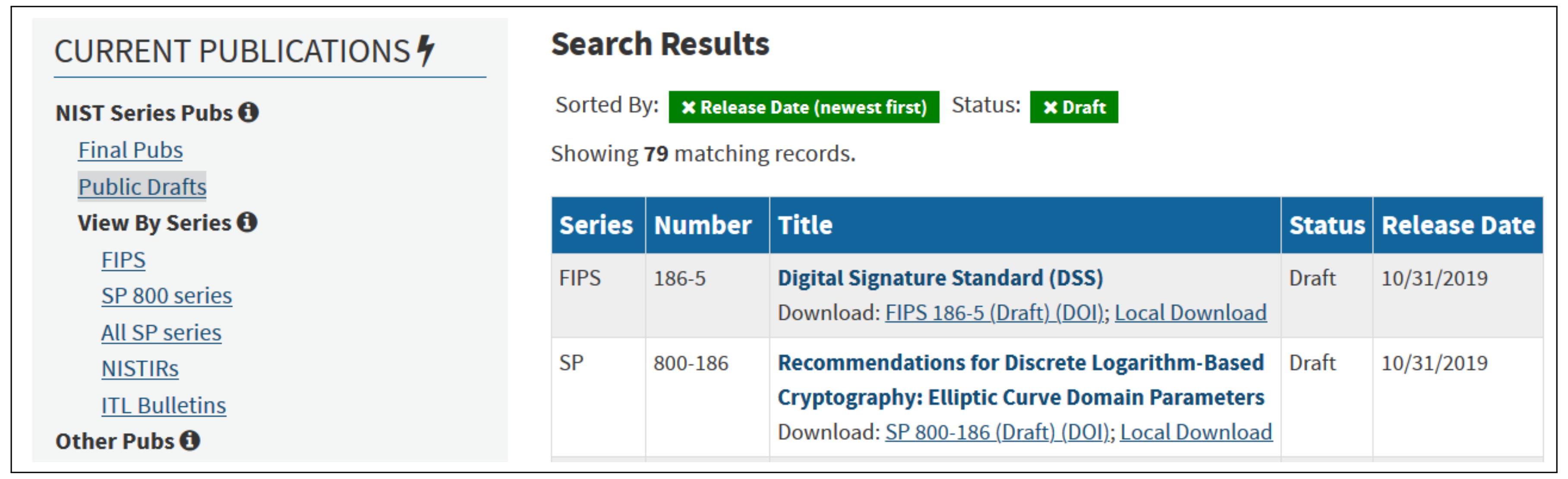
NISTIR
NIST Internal or Interagency Report

ITLB
Information Technology Laboratoty Bulletin

- **FIPS:** Standards & guidelines for federal computer systems (per FISMA).
- **SP 800:** Guidelines, recommendations, technical specs, annual reports.
- **NISTIR:** Reports of research findings; background for FIPS and SPs.
- **ITLB:** Monthly overviews on security and privacy pubs/progs/projects.

Computer Security Resource Center

The CSD maintains the **CSRC**, documenting pubs, projects, news & events.



CURRENT PUBLICATIONS

NIST Series Pubs
Final Pubs
Public Drafts
View By Series
FIPS
SP 800 series
All SP series
NISTIRs
ITL Bulletins
Other Pubs

Search Results

Sorted By: ✖ Release Date (newest first) Status: ✖ Draft

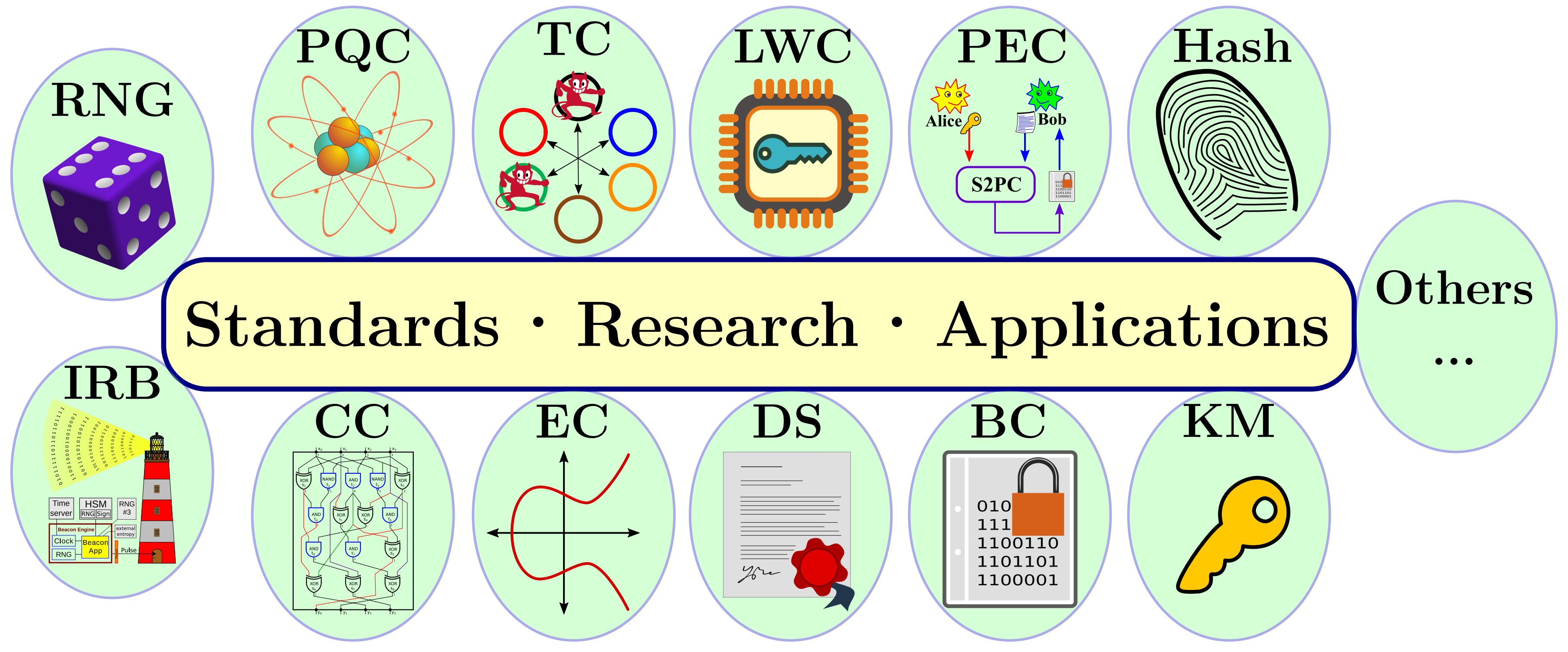
Showing **79** matching records.

Series	Number	Title	Status	Release Date
FIPS	186-5	**Digital Signature Standard (DSS)** Download: FIPS 186-5 (Draft) (DOI); Local Download	Draft	10/31/2019
SP	800-186	**Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters** Download: SP 800-186 (Draft) (DOI); Local Download	Draft	10/31/2019

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

Activities of the Crypto Group

The Crypto group develops new **standards**, performs **research** and develops **applications** that promote adoption of better crypto technologies.



Standards · Research · Applications

Legend: **BC** (Block Ciphers); **CC** (Circuit Complexity); **Crypto** (Cryptography); **DS** (Digital Signatures); **EC** (Elliptic Curves); **IRB** (Interoperable Randomness Beacons); **KM** (Key Management); **LWC** (Lightweight Crypto); **PEC** (Privacy-Enhancing Crypto); **PQC** (Post-Quantum Crypto); **RNG** (Random-Number Generation); **TC** (Threshold Crypto).

More details and examples at https://www.nist.gov/itl/csd/cryptographic-technology

Engagement with stakeholders

NIST Crypto Workshops (recent and soon-to-be):

PQC
- Aug. 2019
- 1st sem. 2021

Post-quantum

LWC
- Nov. 2019
- Oct. 2020

Lightweight

TC
- Mar. 2019
- Nov. 2020

Threshold

Collaboration with external bodies:

- Crypto standards adoption: **ASC X9**; **IEEE**; **IETF**; **ISO**; **TCG**.
- Exploratory work with advanced crypto: **ZKProof**; **HE**.

Recent publications (examples)

- **Signatures:** FIPS 186-5 (Draft): new EdDSA; deprecated finite-fields
- **Post-Quantum Crypto:** NISTIR 8309: candidates for 3rd round
- **Lightweight Crypto:** NISTIR 8268: candidates for 2nd round
- **Threshold Crypto:** NISTIR 8214A: towards criteria
- **Elliptic curves:** SP 800 186 (Draft): Elliptic curve parameters

Other popular topics (examples): AES (FIPS 197); SHA 2/3: (FIPS {180, 202}); Key-Establishment (SP 800-56); RNG (SP 800-90).

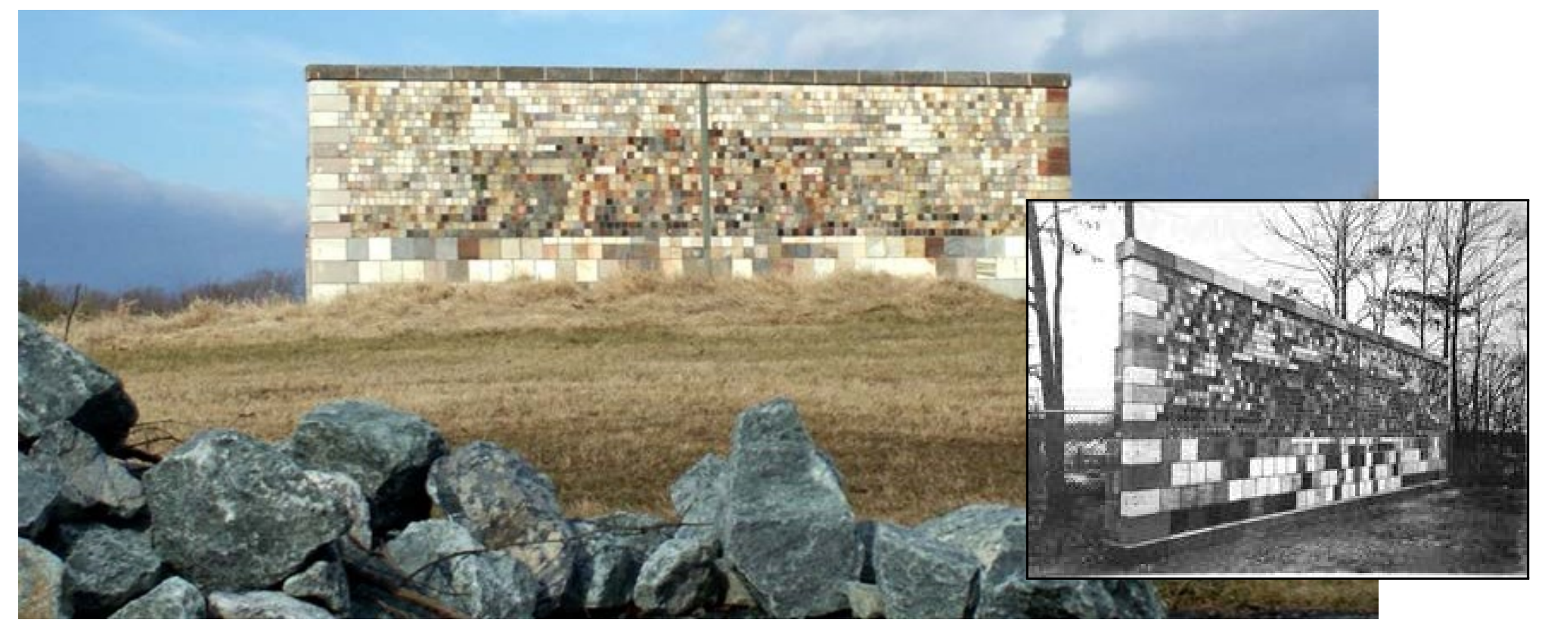
Guidance on cryptography standards:

How to develop, implement and use cryptography standards?

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

Cryptography standards evolve across time:

1. Standards require periodic review (see NISTIR 7977)
2. There is a drive towards “advanced cryptography”
3. Which crypto blocks will resist the test of time?



The NIST Stone Test Wall (2018 / 1948)

Legend: **ASC** (Accredited Standards Committee); **AES** (Advanced Encryption Standard); **ANSI** (American National Standards Institute); **EdDSA** (Edwards-curve Digital Signature Algorithm) **FISMA** (Federal Information Security Management Act); **HE** (Homomorphic Encryption); **IEEE** (Institute of Electrical and Electronics Engineers); **IETF** (Internet Engineering Task Force); **ISO** (International Organization for Standardization); **SHA** (Secure-Hash Algorithm); **TCG** (Trusted Computing Group). **ZK** (Zero Knowledge).

Poster produced for presentation at the NIST-ITL Virtual Science Day 2020 (October 29).
Poster prepared by Luís Brandão: Foreign Guest Researcher at NIST (Contractor via Strativia).
External cliparts are from clker.com, included here under a fair-use or free-use license expectation.