

NIST cryptography standards

The NIST Cryptographic Technology Group (**CTG**) develops Internationally renowned crypto standards.



CTG **collaboration** with Standards Developing Organizations (**SDOs**) improves the Int'l standards ecosystem and U.S. competitiveness in the global marketplace.

NIST ↔ SDOs

- **SDOs adopt NIST crypto standards.** Thus, vendors with products using NIST standards to meet U.S. Gov. needs can also enter Int'l markets.
- **NIST adopts SDOs' best-practice standards.** Thus, vendors in some industries get abler to operate in settings requiring NIST-approved standards.

Win-win: Active collaboration helps with:

- sharing expertise; enhancing resource efficiency;
- producing widely-accessible interoperable standards.

Poster produced for the NIST-ITL Science Day 2021 (October 28), by Luís T. A. N. Brandão (at NIST as a contractor from Strativia) and Lily Chen.

CTG collaborations with SDOs

The interaction and impact vary with the SDO (usually in a focused sub-committee). Each interaction has a motivating application area to justify the used resources.

SDO	Subcommittee or context
	JTC1/SC27/WG2: Cryptography and Security
	802.11 Wireless Fidelity (WiFi) service
	ASC-X9F1: PKC for Financial Services Industry
	Internet Protocols (TLS, IPsec, ...)
	TCG "Root of trust" for Hardware Security

- SDOs have adopted main NIST crypto standards.
- CTG only participates in selected sub-committees.
- CTG deals with primitives, protocols and security.

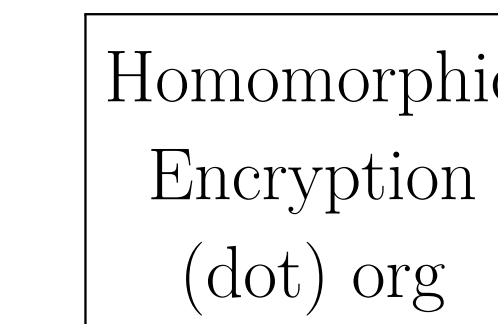
Legend. ASC: Accredited Standards Committee. IEC: International Electrotechnical Commission. IEEE-SA: Institute of Electrical and Electronics Engineers — Standards Association. IETF: Internet Engineering Task Force. IPsec: Internet Protocol Security. ISO: International Organization for Standardization. JTC: Joint Technical Committee. KeyGen: Key Generation. PKC: Public- Key Cryptography. RNG: Random Number Generation. SC: subcommittee. TCG: Trusted Computing Group. TLS: Transport Layer Security. WG: Working Group.

Emerging initiatives

The CTG also engages in industry+academia lead efforts:



ZKProof. Initiative toward ZKP standards. Since 2019, CTG contributes to the ZKProof Community Ref. and is part of editors' team.



HomomorphicEncryption. The initiative proposes a standard for FHE. CTG collaborates since 2017, attending workshops.

A future looking forward

- Promote adoption of upcoming NIST PQC and LWC standards in Int'l standards for diverse applications.
- Collaborate with Int'l experts to standardize advanced techniques from PEC and Threshold cryptography.
- Continue cutting-edge research and lead crypto standards development for information security needs.

Find more info about the CTG at <https://www.nist.gov/itl/csd/cryptographic-technology>

Find NIST crypto publications (e.g., FIPS, SP 800) at <https://csrc.nist.gov/publications>

Legend. FHE: Fully Homomorphic Encryption. FIPS: Federal Information Processing Standards. Int'l: International. LWC: Lightweight Cryptography. PEC: Privacy-Enhancing Cryptography. PQC: Post-Quantum Cryptography. Ref.: Reference. SP 800: Special-Publications in Computer Security. ZKP: Zero Knowledge Proof.