Public Calls Toward Standards & Guidelines for Crypto Primitives

Cryptographic Technology Group, Computer Security Division

INFORMATION TECHNOLOGY LABORATORY

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

NIST Cryptography Standards

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

Open calls. NIST has several approaches to develop cryptography standards. One involves issuing timed open calls for contributions, followed by intense public analysis.

This poster lists some calls (past, recent, soon) that resulted / intend to result in new standards/guidelines.

Past Calls → **Recent/Soon Calls**

Advanced Encryption Standard (AES)

- Block ciphers allow confidential communication
- AES is standardized in FIPS 197, since 2001
- Rijndael selected after 5-year analysis of 15 designs
- AES superseeded the Data Encryption Standard

Post-Quantum Cryptography (PQC)

- PQC intends to resist quantum attacks (which break existing public-key crypto in FIPS 186, SP 800-56 A/B)
- PQC Call (2016): PKE/KEMs, digital signatures
- PQC rounds (R): $82 \xrightarrow{R0} 69 \xrightarrow{R1} 26 \xrightarrow{R2} 7{+}8$
- 2022: Round 3 chose 4 algorithms for standardization: CRYSTALS-{Kyber, Dilithium}, Falcon, SPHINCS+
- 2024: The first PQC standards expected (FIPS)

Secure Hash Algorithm 3 (SHA3)

- Hash functions are essential for authentication
- SHA3 is standardized in FIPS 202, since 2015
- Keccak selected by NIST hash function competition
- The Int'l competition received 51 candidates in 2008

Legend. AEAD: Authenticated encryption with associated data. **FIPS**: Federal Information Processing Standard. **Int'l**: International. **KEM**: key-encapsulation method. **NISTIR**: NIST internal report. **PKE**: public-key encryption. **RNG**: random number generation. **R0**: round 0 (period between submissions and approval of packages for the first round). **SDO**: Standards Development Organization. **SP 800**: Special publication in computer security.

Lightweight Cryptography (LWC)

- Lightweight primitives are important for constrained environments (e.g., low energy, power, latency)
- LWC Call (2018): Authenticated Encryption with Associated Data (AEAD), with optional hashing
- LWC rounds (R): $57 \xrightarrow{R0} 56 \xrightarrow{R1} 32 \xrightarrow{R2} 10$
- Round 3 started in 2021 with 10 finalists
- Announcement of "winner(s)" expected for late 2022

Multi-party Threshold Crypto (MPTC)

- Threshold crypto allows operations on distributed key
- 2023: Upcoming Call for Threshold Schemes
- Scope: thresholdize primitives needed for signing, encryption/decryption, key-agreement, key-generation
- Aims at future guidelines and recommendations, highlighting best practices and sound approaches

Poster presented by Luís Brandão and Lily Chen at the NIST-ITL Science Day 2022 (October 24th). Poster produced by joint collaboration between Luís Brandão (Foreign Guest Researcher at NIST, contractor from Strativia), Lily Chen, Dustin Moody, and Meltem Sonmez Turan.