

Advances in NIST Symmetric-Key Standards: Ascon, Accordion, and Wide-AES

Meltem Sönmez Turan, NIST



NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

MPTS 2026: NIST Workshop on Multi-Party Threshold Schemes 2026
January 28, 2026

Scope of the talk

Lightweight Cryptography

- Overview of the standardization effort
- Post-standardization activities

Wide-Block AES

- Motivation and intended use cases
- NIST's plan to standardize **Rijndael-256**

Accordion Ciphers

- New mode, three approaches
- Current status

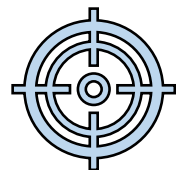


“Lightweight” refers to implementation cost, not reduced security.



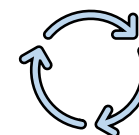
GOAL

Standardize **secure and efficient** symmetric-key primitives for constrained environments



SCOPE

Authenticated Encryption and (optional) hashing for constrained software and hardware environments



PROCESS

Open, international, public competition-like process with multiple rounds similar to AES, SHA3 standardization

Timeline of the Standardization Process



Initial Phase (July 2015 – August 2018)

- Two workshops
- **NIST IR 8114** Report on lightweight cryptography



Submission Call (Aug. 2018 – April 2019)

Submission requirements and evaluation criteria for the LWC standardization process.



Round 1 (April – August 2019)

- 56 round-1 candidates
- **NIST IR 8368** – the selection of 32 second-round candidates.



Round 2 (August 2019 – March 2021)

- 32 round-2 candidates
- Two workshops
- **NIST IR 8369** explains the selection of 10 finalists.



Final Round (March 2021 – June 2023)

- 10 finalists
- One workshop
- **NIST IR 8369** explains the selection of Ascon family.



Standardization (July 2023 - August 2025)

- One workshop
- **SP 800-232** published August 2025.

SP 800-232 standard includes

- **Ascon-AEAD128** (Authenticated Encryption with Associated Data)
 - 128-bit key, 128-bit nonce, and 128-bit tag
 - Optional nonce-masking variant supporting 256-bit keys
- **Ascon-Hash256** (Cryptographic hash function)
 - 256-bit hash output size
- **Ascon-XOF128** and **Ascon-CXOF128** (eXtendable Output Functions)
 - Arbitrary length output
 - Ascon-CXOF supports customization

128-bit security strength across primitives.

Deployment and Adoption

- Ascon is transitioning from standardization to real-world deployment
- Adoption across software libraries and hardware implementations
- Alignment with international efforts (ISO, IETF)

Validation and Assurance

- Supporting cryptographic algorithm validation for Ascon implementations
- Enabling conformance testing to promote correct and interoperable deployments
- Providing assurance for federal, commercial, and international users

Maintenance

- Ongoing maintenance to ensure robustness and interoperability
- Incorporating new cryptanalysis and implementation feedback

Extending Functionality

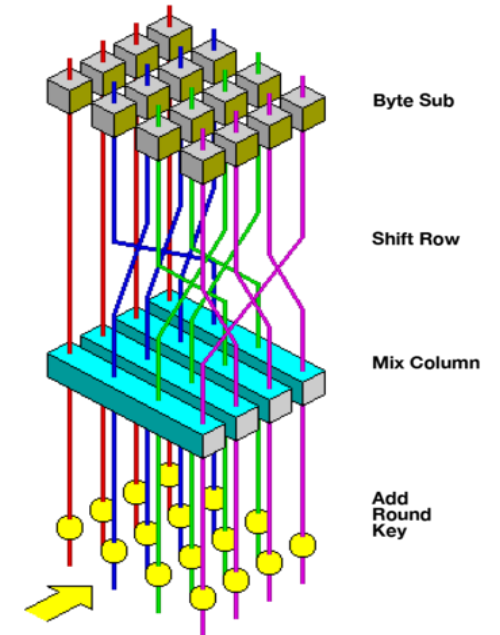
- Exploring standardization of additional primitives based on the Ascon design, including:
 - Dedicated Message Authentication Codes (MACs)
 - Variable-output-length pseudorandom functions (PRFs)
 - Deterministic Random Bit Generators (DRBGs), etc.

Advanced Encryption Standard

- Designed by Daemen and Rijmen as Rijndael
- Specified in **FIPS 197** Advanced Encryption Standard (2001)
- Widely adopted across industries and protocols
- Hardware acceleration (AES-NI) enables high performance.
- Significant economic impact
(see [“The Economic Impacts of the Advanced Encryption Standard, 1996 – 2017”](#))

Variants:

- **AES-128**: 128-bit key, 128-bit block
- **AES-192**: 192-bit key, 128-bit block
- **AES-256**: 256-bit key, 128-bit block



*AES round function
(figure from Wikipedia)*

Supported key sizes:
128, 160, 192, 224, 256

Supported block sizes:
128, 160, 192, 224, 256

Block Cipher Modes of Operations (SP 800-38 Series)

NIST has standardized several modes for AES.

Confidentiality-Only Modes

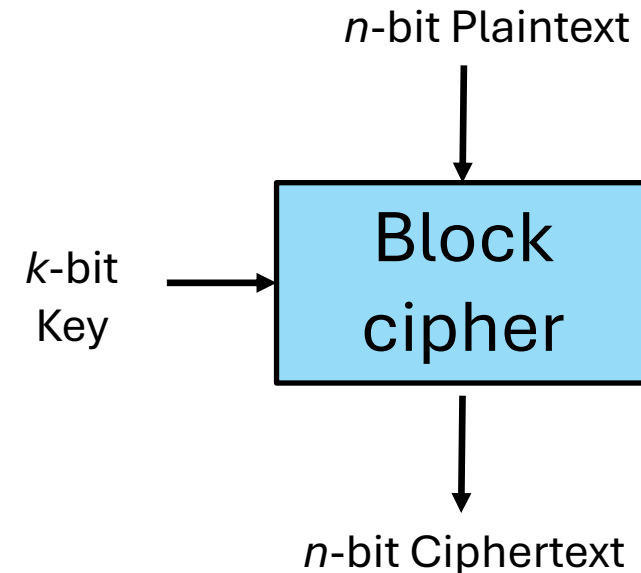
- SP 800-38A & Addendum
- ECB, CBC, CFB, OFB, CTR
- CBC variants: CBC-CS1, CBC-CS2, CBC-CS3

Authentication & AEAD

- SP 800-38B — CMAC (Message Authentication Code)
- SP 800-38C — CCM (AEAD: encryption + authentication)
- SP 800-38D — GCM (AEAD) and GMAC (MAC)

Specialized Use Cases

- SP 800-38E — AES-XTS (storage encryption)
- SP 800-38F — Key wrapping: AES Key Wrap (KW), AES KW with Padding, TDEA Key Wrap (TKW)
- SP 800-38G — Format-Preserving Encryption (FF1, FF3)



In 2021, the **NIST Crypto Publication Review Board** initiated a review of AES and modes standards.

Key findings

- Nonce misuse in AES-GCM remains a major risk
- Data limits are increasingly relevant (AES-GCM limits plaintext to 2^{39} – 256 blocks per key/IV)
- Security expectations have evolved: growing demand for key- and context-committing AEAD

Implications:

- Correct usage alone is not sufficient for long-term robustness
- New constructions are needed to better tolerate misuse and scale

NIST Directions:

- Wide-block primitives (e.g., AES-based constructions with larger block size)
- Misuse-resistant (e.g., AES-GCM-SIV) and committing AEAD
- Alternative design approaches beyond traditional AES-based modes

NIST Decision: Standardizing a Wider AES Variant



NIST plans to develop a revision of FIPS 197 to include Rijndael-256.

Motivation

- Support for larger data under long-lived keys
- 128-bit block sizes impose birthday-bound limits on data processing
- Larger blocks offer wider internal state and expanded tweak/nonce space

What is Being Standardized

- Rijndael with a **256-bit block size** and fixed **256-bit key**
- Same design family and round structure as AES

Complements the current AES algorithms, does not replace!

Accordion Mode: A new direction for block cipher modes

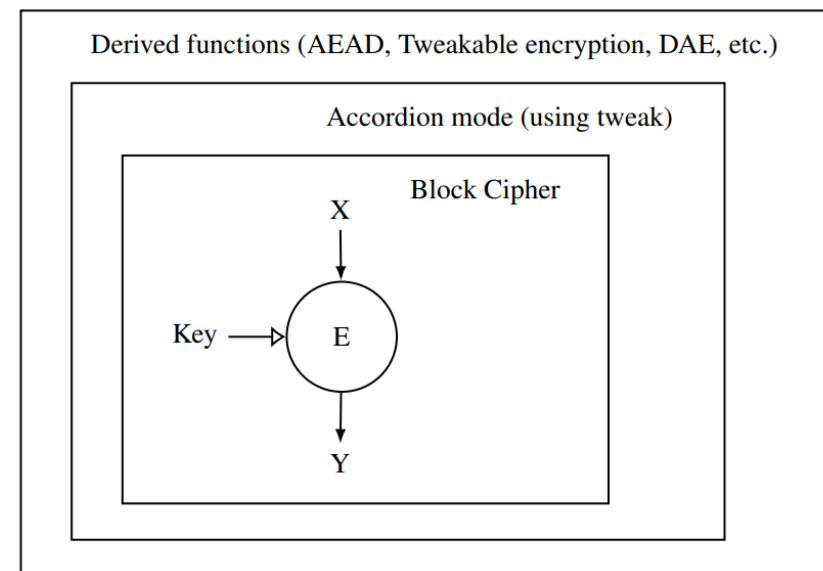
- A block-cipher mode that behaves like a cipher on variable-length messages
- Built as a tweakable, strong pseudorandom permutation

What it enables

- Flexible handling of short and long messages
- Integrated support for associated data (nonce, tweak, context)
- Derivation functions to support AEAD and deterministic authenticated encryption, tweakable encryption etc.

Why It Matters

- Improves robustness against misuse
- Supports stronger security guarantees than existing SP 800-38 modes



NIST Proposal: Three Accordions



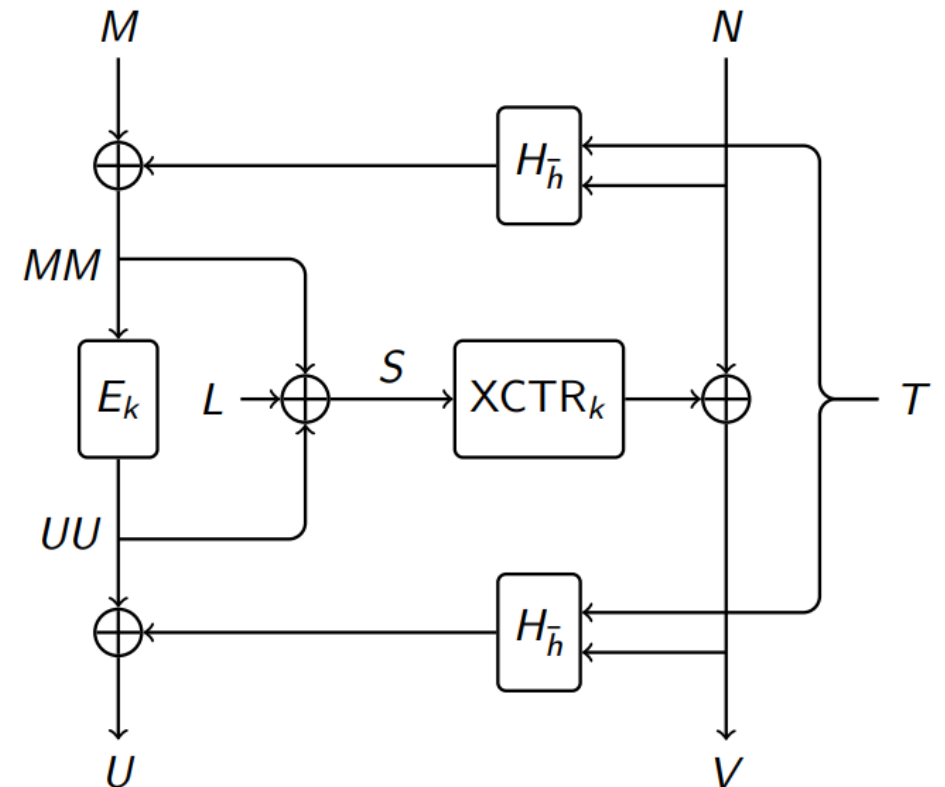
NIST proposes three general-purpose accordions:

Acc128 – Typical usage	Acc256 – Larger block variant	BBBAcc – Extended usage
<ul style="list-style-type: none">- Targets birthday-bound security- Built from AES- Designed for broad deployment and efficiency	<ul style="list-style-type: none">- Targets typical usage with a wider block.- Built from Rijndael-256- Enables larger state and extended tweak space	<ul style="list-style-type: none">- Targets beyond-birthday-bound security- Built using AES- Designed for large data volumes

Process: Collaborative process with the crypto community

NIST proposes to develop variants of the **HCTR2** technique for these accordions.

- Designed by Crowley, Biggers, and Huckleberry (Google) for length-preserving encryption (2021)
- Transforms a fixed-block cipher into a **tweakable, variable-length authenticated encryption**
- Hash-Encrypt-Hash structure
- Combines **universal hashing** with **block cipher encryption**. Hashing uses Polyval, encryption uses XOR-based counter mode
- Supports tweaks for nonce and AD



- Ascon is now standardized, providing secure and efficient lightweight cryptography for constrained environments.
- Wide-AES (Rijndael-256) expands the AES family, mainly to address data limits.
- Accordion modes represent the next generation of block cipher modes, offering flexibility, misuse resistance, and stronger security guarantees.

1. NIST SP 800-232 Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions
<https://doi.org/10.6028/NIST.SP.800-232>
2. NIST IR 8552 Requirements for Cryptographic Accordions <https://doi.org/10.6028/NIST.IR.8552>
3. NIST IR 8537 NIST Workshop on the Requirements for an Accordion Cipher Mode 2024: Workshop Report <https://doi.org/10.6028/NIST.IR.8537>
4. NIST IR 8459 Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series
<https://doi.org/10.6028/NIST.IR.8459>

CONTACT US

meltem.turan@nist.gov

Email forum: **Block cipher modes – ciphermodes-forum@list.nist.gov**
Lightweight Cryptography – lwc-forum@list.nist.gov