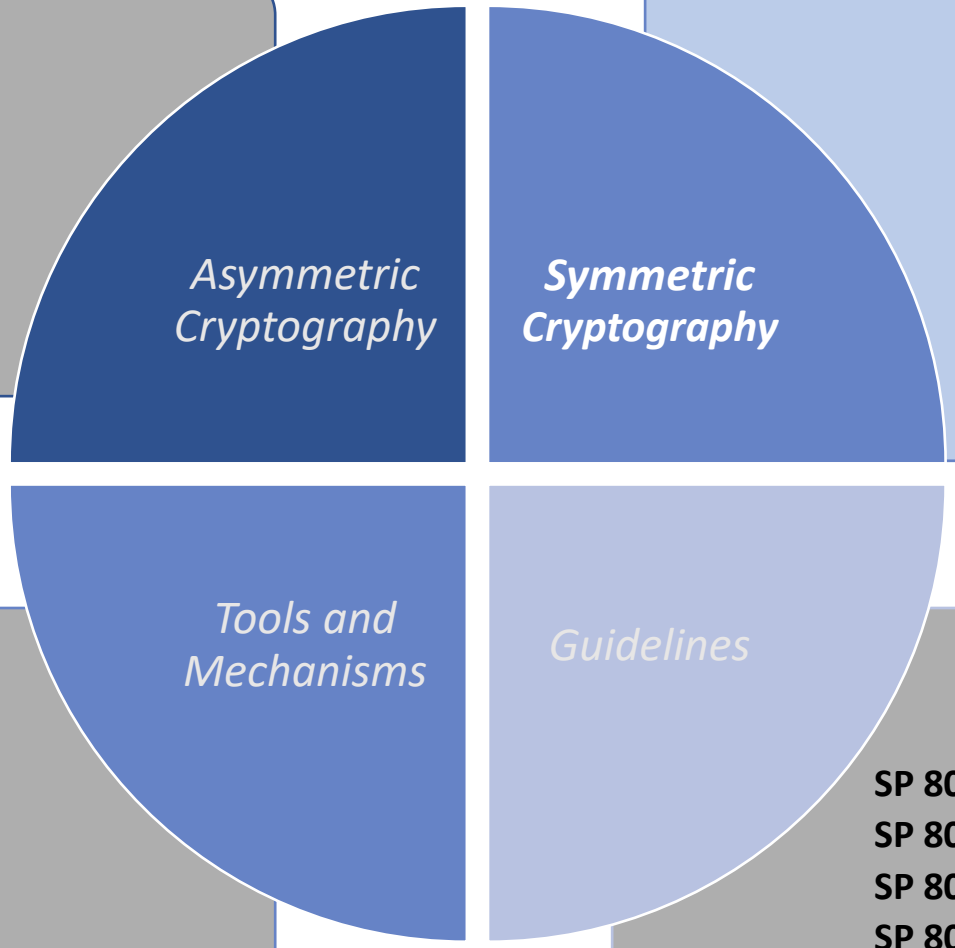
NIST Options in for Encryption Algorithms and Modes of Operation

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

Andrew Regenscheid
Andrew.Regenscheid@nist.gov

Standards and Guidelines



Digital Signatures
- **FIPS 186**- RSA/ECDSA/EdDSA
- **FIPS 204**- ML-DSA
- **FIPS 205**- SLH-DSA

Key Establishment
- **SP 800-56A**- DH/ECDH
- **SP 800-56B**- RSA
- **FIPS 203**- ML-KEM

Block Ciphers
- **FIPS 197**- AES
- **SP 800-38**- Modes

Hash Functions
- **FIPS 180**- SHA2
- **FIPS 202**- SHA3
- **SP 800-185**- Derived Func.

FIPS 198- HMAC

Random Number Generation
- **SP 800-90A**- DRBG Algorithms
- **SP 800-90B**- Entropy Assessment
- **SP 800-90C**- RBG Constructions

Key Derivation Functions
- **SP 800-108**- KDFs using PRFs
- **SP 800-135**- App.-specific KDFs

SP 800-52- TLS
SP 800-57- Key Management
SP 800-89- Dig. Sig. Assurances
SP 800-107- Hash Applications
SP 800-133- Key Generation

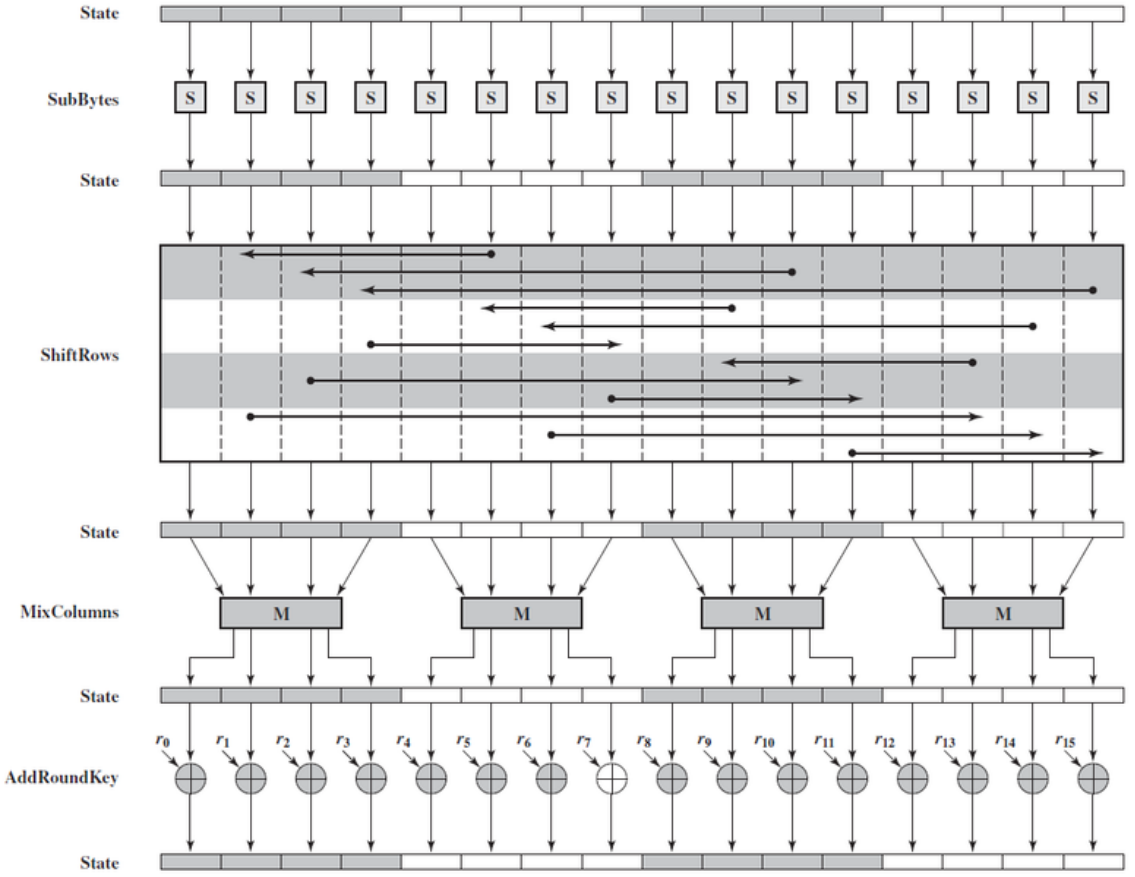
Block Ciphers- Rijndael-256

Identified Need:

- Wide block cipher to support higher data limits
- Reuse AES Instructions → ***Rijndael-256-256***

Decisions:

- What additional analysis is needed?
- Should the key schedule be revised?
- Is there a need for a tweakable block cipher?
- New or adapted modes?



AES Round Function

Figure: *Author: Jeongysu Source: Wikimedia Commons*

Modes of Operation

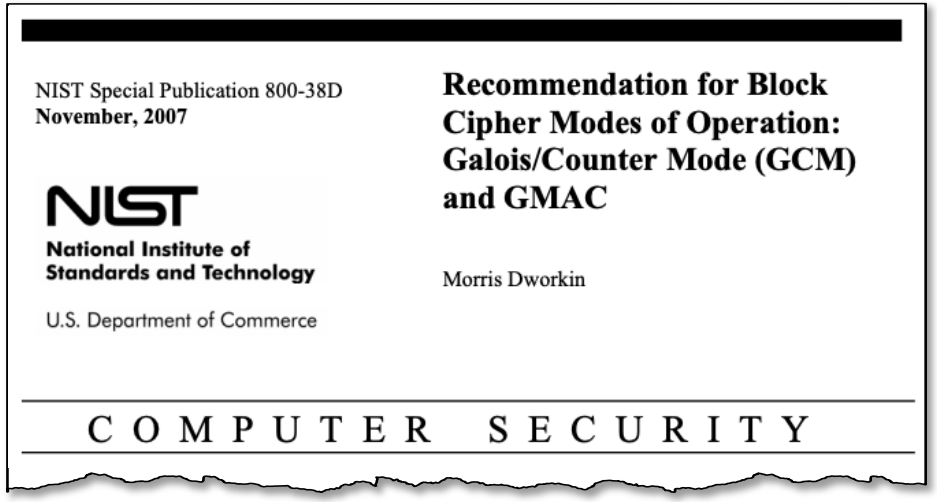
Identified Need:

- Support higher data limits
- Provide misuse resistance

Potential Short-term Options

- *Existing Modes*
  - Potential extensions– *e.g.,* DNDK-GCM
  - Revised guidance in 800-38 series
- *Submitted Modes*
  - *e.g.,* AES-GCM-SIV (RFC 8452)

Challenge: No solution that meets all needs



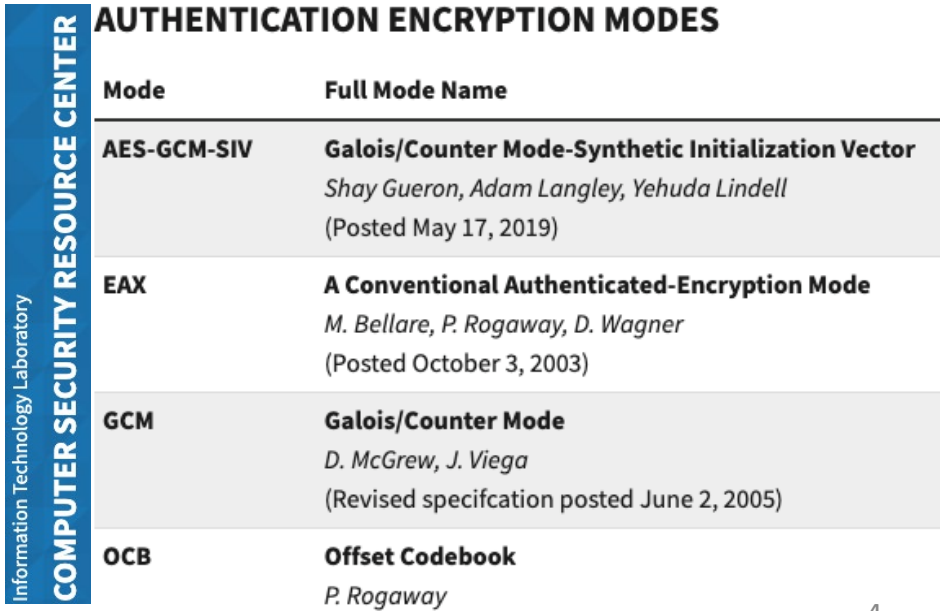
NIST Special Publication 800-38D
November, 2007

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

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

Morris Dworkin

COMPUTER SECURITY



Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

AUTHENTICATION ENCRYPTION MODES

Mode	Full Mode Name
AES-GCM-SIV	**Galois/Counter Mode-Synthetic Initialization Vector** *Shay Gueron, Adam Langley, Yehuda Lindell* (Posted May 17, 2019)
EAX	**A Conventional Authenticated-Encryption Mode** *M. Bellare, P. Rogaway, D. Wagner* (Posted October 3, 2003)
GCM	**Galois/Counter Mode** *D. McGrew, J. Viega* (Revised specifcation posted June 2, 2005)
OCB	**Offset Codebook** *P. Rogaway*

Keccak-Based AEAD

Identified Need:

- Authenticated encryption mode from Keccak permutation
- Reuse implementation components from SHA-3 and SHAKE *(and new PQC algorithms)*

Decisions:

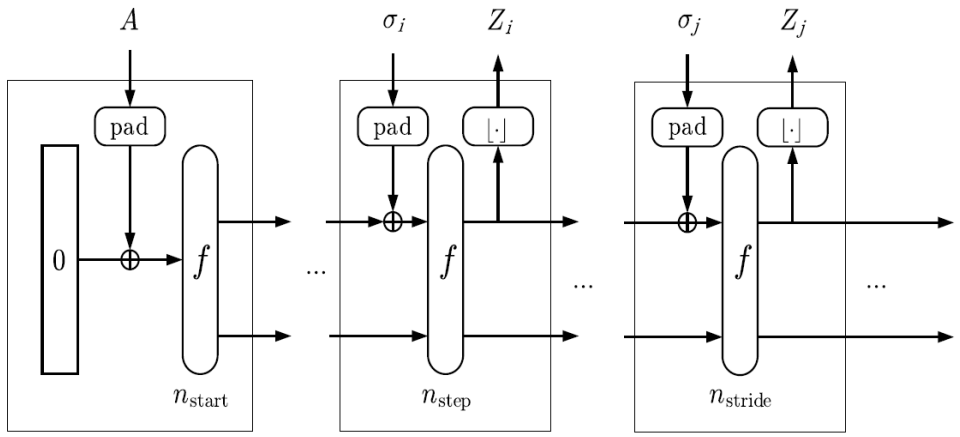
- Several constructions have been proposed– which one?
- What size permutation?
- How many rounds?
- Features? *e.g.,* parallelizability?

FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY



Thank you