Overview of the NIST Block Cipher Modes Project

Meltem Sönmez Turan and Donghoon Chang
NIST Computer Security Division

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

NIST Workshop on the Requirements for an Accordion Cipher Mode
June 20, 2024

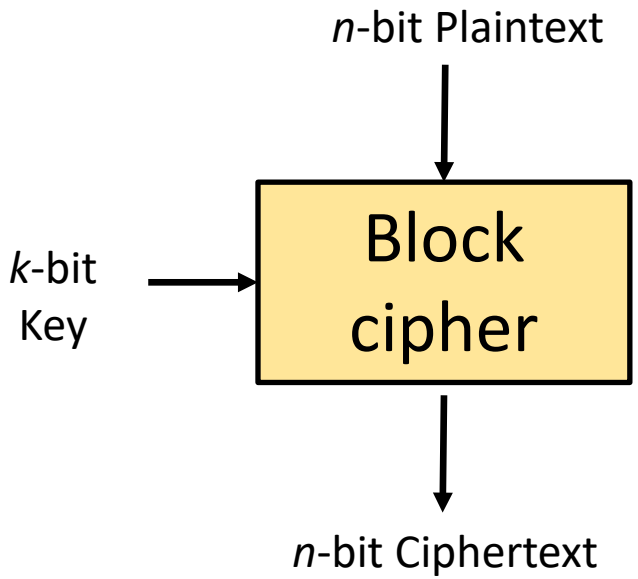
Overview

Block ciphers & modes

SP 800-38 series

Feedback received

NIST-Approved Block Ciphers



WITHDRAWN

Data Encryption Standard (DES):

- Specified in FIPS 46 (1977), withdrawn in 2005.
- FIPS 81 (1980) specified ECB, CBC, CFB and OFB

Skipjack:

- Specified in FIPS 185 (1994), withdrawn in 2015
- Used with modes from FIPS 81

TripleDES:

- Specified in FIPS 46-3, later in SP 800-67 (2004), withdrawn in 2023

Advanced Encryption Standard:

- Specified in FIPS 197(2001) reviewed[1] & updated in 2023
- Widely adopted, with a significant impact on economy [2]

1. *Crypto Publication Reviews*
2. Leech et al., *The Economic Impacts of the Advanced Encryption Standard*, 2018

Advanced Encryption Standard (AES)

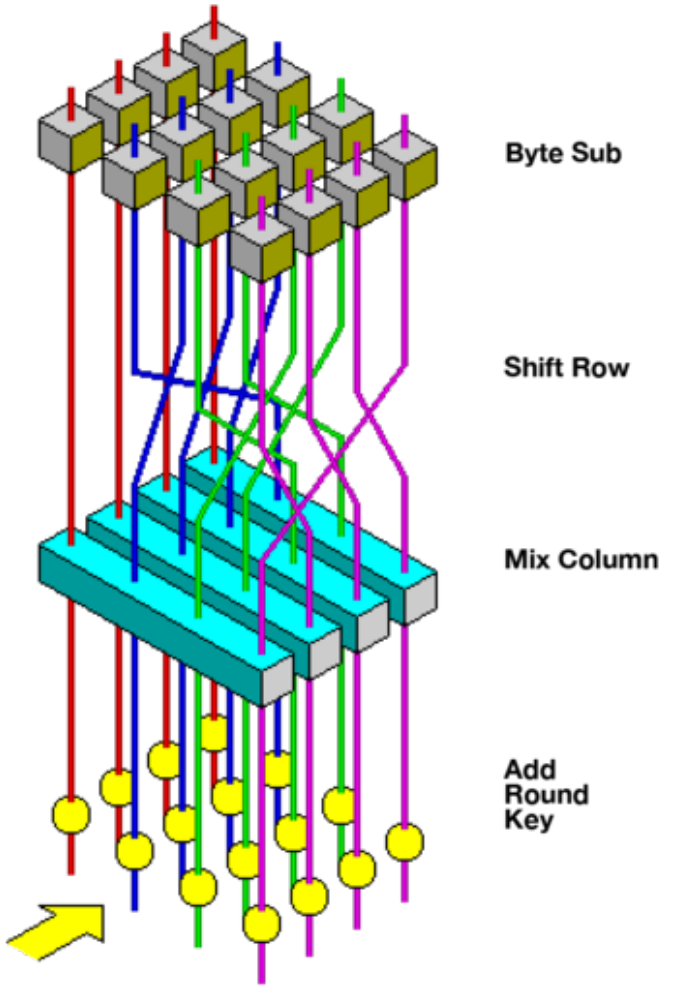
Rijndael is designed by Rijmen and Daemen.

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

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

FIPS 197 specifies three variants

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



AES round function

(figure from Wikipedia)

Block Cipher Modes of Operation

A mode of operation for block ciphers describes a method to process arbitrary-length inputs under a single key.

Goal: provide a cryptographic functionality like confidentiality, authentication, authenticated encryption, etc. using block ciphers

Typically, modes include simple operations (such as message padding, XOR operation, bit manipulations, finite field arithmetic).

Choosing the right mode is crucial for security and efficiency, depending on the application's requirements.

- Efficiency, flexibility, provable security (e.g., PRP, strong-PRP, ideal cipher assumptions), the gap between known attacks and proven bounds, different inputs (nonce, tweak, or IV), the impact of nonce reuse, robustness, etc.

NIST Special Publication 800-38 Series

- SP 800-38A & Addendum: Confidentiality-only modes ECB, CBC, CFB, OFB, CTR. Addendum includes three CBC variants: CBC-CS1, CBC-CS2, CBC-CS3
- SP 800-38B: Cipher-based Message Authentication Code CMAC
- SP 800-38C: Counter with Cipher Block Chaining-Message Authentication Code (CCM)
- SP 800-38D: Galois/Counter Mode (GCM) and its specialization GMAC to generate a Message Authentication Code (MAC).
- SP 800-38E: AES-XTS mode for confidentiality on storage devices
- SP 800-38F: Authenticated encryption for key wrapping: AES Key Wrap (KW), the AES Key Wrap with Padding (KWP), and TDEA Key Wrap (TKW)
- SP 800-38G: Format preserving encryption FF1, FF3

Development of Block Cipher Modes

- Open invitation to submit block cipher modes to be considered for standardization
- Submissions are posted for public review
- NIST decides to pursue a proposal
- NIST develops a draft Special Publication for public review in consultation with submitters
- NIST decides whether to
  - Finalize and publish the document
  - Revise the draft for further public review
  - Withdraw proposal

Timeline

Pre-AES
- 1977 FIPS 46 DES
- 1980 FIPS 81 ECB, CBC, CFB, OFB, CBC-MAC, CFB-MAC
- 1998 FIPS 46-3 Triple DES

2000-2020
- 2000 Block Cipher Modes Workshop I
- 2001 FIPS 197 AES (updated in 2023)
- 2001 SP 800-38A ECB, CBC, CFB, OFB, CTR
- 2001 Block Cipher Modes Workshop II
- 2004 SP 800-38C CCM (updated in 2007)
- 2005 SP 800-38B CMAC (updated in 2016)
- 2007 SP 800-38D GCM & GMAC
- 2010 SP 800-38E XTS-AES
- 2010 SP 800-38A addendum CBC-CS variants
- 2012 SP 800-38F KW, KWP, TKW
- 2016 SP 800-38G Format-Preserving Encryption FF1, FF3 (Revision draft, 2019)

2020 - …
- 2023 Third NIST Workshop on Block Cipher Modes of Operation
- 2023 Report on the Block Cipher Modes
- 2024 Discussion Draft for the NIST Accordion Mode Workshop 2024
- 2024 NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

SP 800-38A

Title: Recommendation for Block Cipher Modes of Operation: Methods and Techniques

Addendum: Three Variants of Ciphertext Stealing for CBC Mode

Scope: Specifies the following *confidentiality* modes:

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)

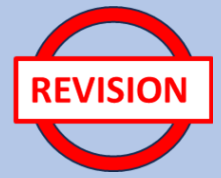
History:

- Published in December 2001
- Addendum published in October 2010

Revision Plans:

NIST initiated a review of SP 800-38A in May'21 and proposed to **revise** the publication to

- limit the approval of ECB mode to instances that are specifically allowed by other NIST standards (e.g., Challenge-response protocol in SP 800-73r4)
- clarify the requirements for the IVs and counter blocks
- provide guidance on the importance of incorporating authentication, where feasible
- incorporate the content of the addendum into the revision

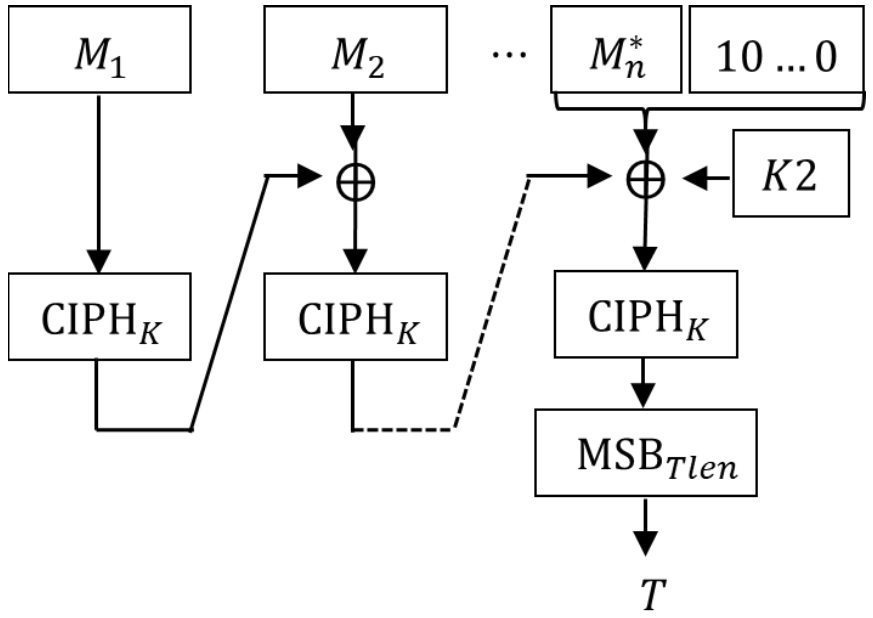


SP 800-38B

Title: Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication

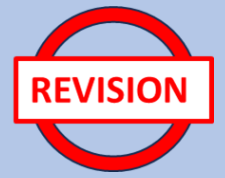
Scope: Block-cipher-based message authentication code (MAC), called CMAC

History:
- Published in May 2005
- Updated in October 2016 (no major technical change)



Revision Plans:
NIST initiated a review of SP 800-38B in June 2024. Public comments due: September 13, 2024.

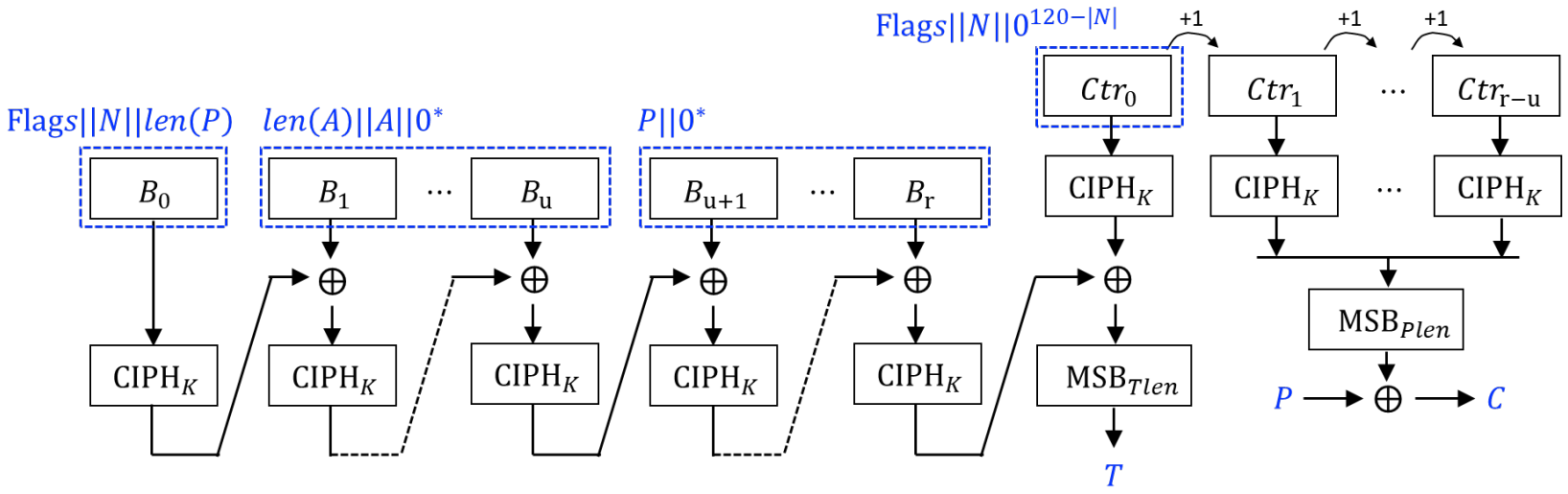
Questions to reviewers:
- Should the standard include a minimum tag length (such as 64-bits or more)?
- If not, what conditions/requirements should be specified for the use of shorter authentication tags for CMAC?



SP 800-38C

Title: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality

Scope: Specifies the block-cipher based Counter with Cipher Block Chaining-Message Authentication Code (CCM).



History:

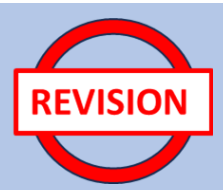
- Published in May 2004
- Updated in July 2007 (includes an errata update for test vectors)

Revision Plans:

NIST initiated a review of SP 800-38C in June 2024. Public comments due: September 13, 2024.

Questions to reviewers:

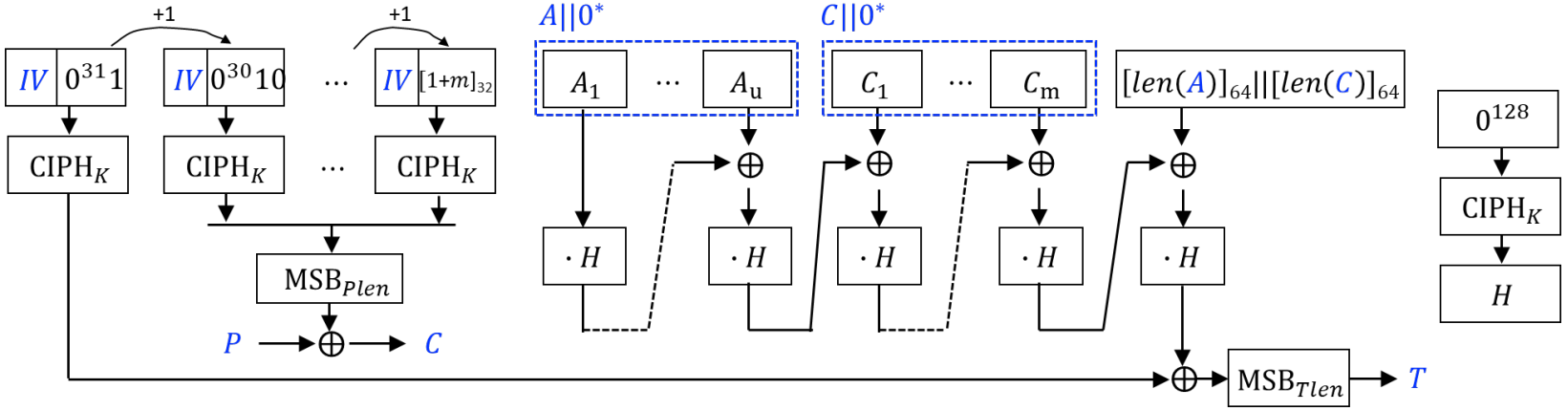
- Should the standard include a minimum tag length (such as 64-bits or more)?
- If not, what conditions/requirements should be specified for the use of shorter authentication tags for CCM?



SP 800-38D

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

Scope: GCM for AEAD, and GMAC to generate a MAC.



History:

- Published in November 2007

Revision Plans:

NIST initiated a review of SP 800-38D in May'21 and proposed to *revise* the publication to

- remove support for authentication tags whose lengths are less than 96 bits,
- clarify that the construction of initialization vectors (IVs) for GCM in the Transport Layer Security (TLS) 1.3 protocol is approved,
- clarify the guidance in connection with the IV constructions.

REVISION

SP 800-38E

Title: Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices

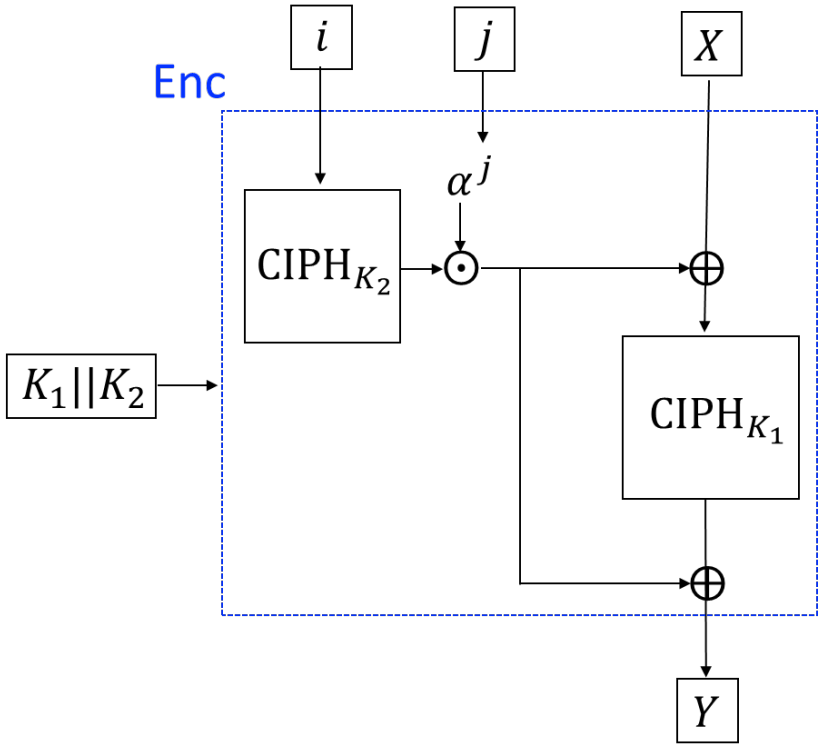
Scope: approves the XTS-AES mode of the AES algorithm by reference to IEEE Std 1619-2007.

Full specification of the XTS-AES is not included in SP 800-38E.

History:
- Published in January 2010

Revision Plans:
NIST initiated a review of SP 800-38E in 2021 and proposed to *revise* the publication to
- explore the feasibility of providing the full specification.
- Refer to the latest version of the external standard

REVISION



SP 800-38F

Title: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

Scope: specifies cryptographic methods for "key wrapping," (i.e., the protection of the confidentiality and integrity of cryptographic keys).

- AES Key Wrap (KW)
- AES Key Wrap With Padding (KWP)
- TKW mode using Triple Data Encryption Algorithm (TDEA) for legacy applications.

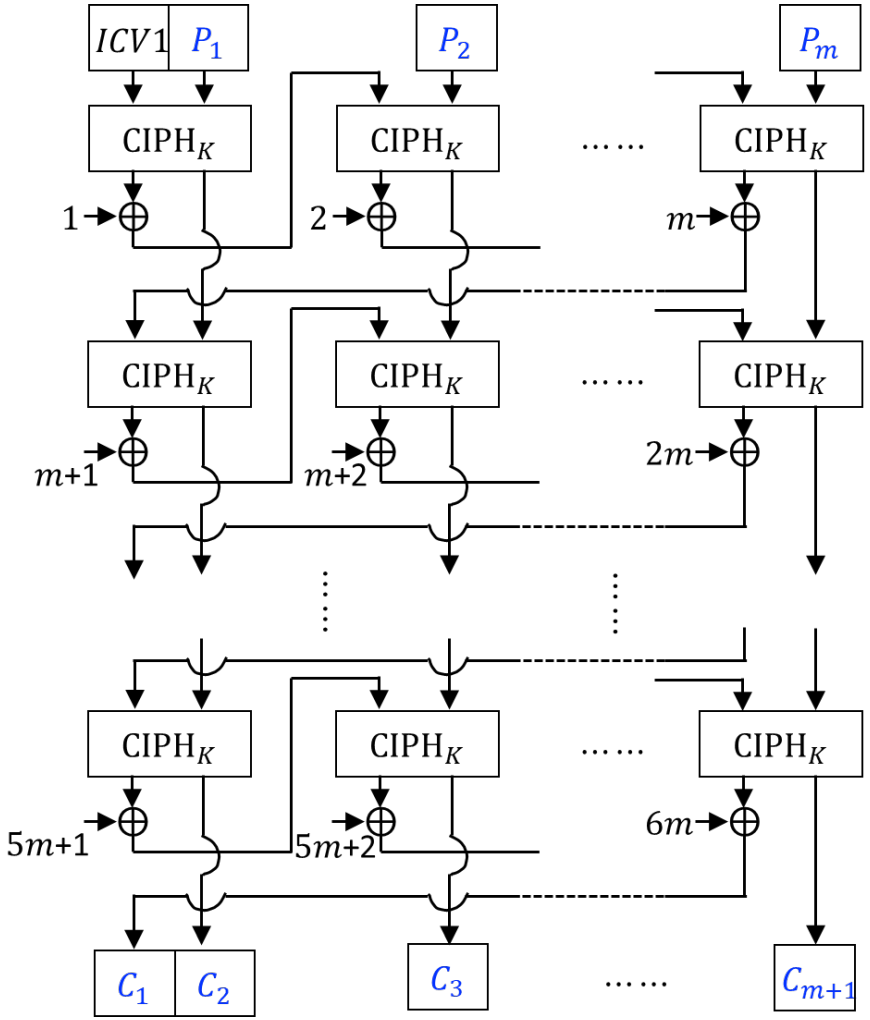
History:

- Published in December 2012

Revision Plans:

Review not initiated yet.

REVISION



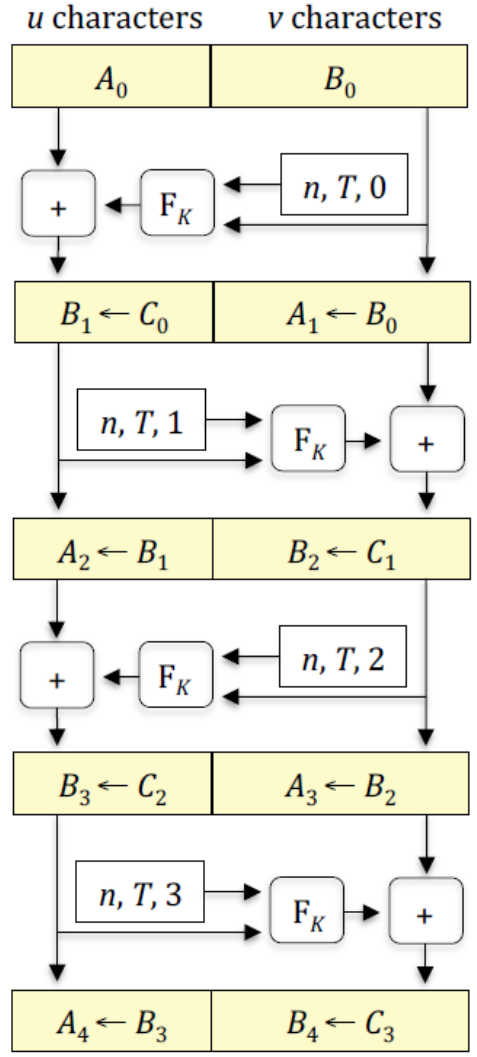
SP 800-38G

Title: Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption

Scope: Specifies two format-preserving encryption modes:
- FF1
- FF3

History:
- Published in March 2016
- Updated in August 2016
- Draft Revision 1 was published in 2019 to address potential vulnerabilities, when the domain size is too small. (tweak size parameter is reduced to 56 bits). Revised FF3 is named FF3-1. Minimum domain size is updated to 1 million.

Revision Plans:
Final version of Revision 1 will be published.



Summary of Feedback

Issues with AES-GCM:

- Nonce misuse issue (96-bit nonce not allowing the use of random nonces)
- Maximum plaintext length of 2^{39}-256
- Not provide key commitment
- Not suitable to use short tags

Some of the suggestions:

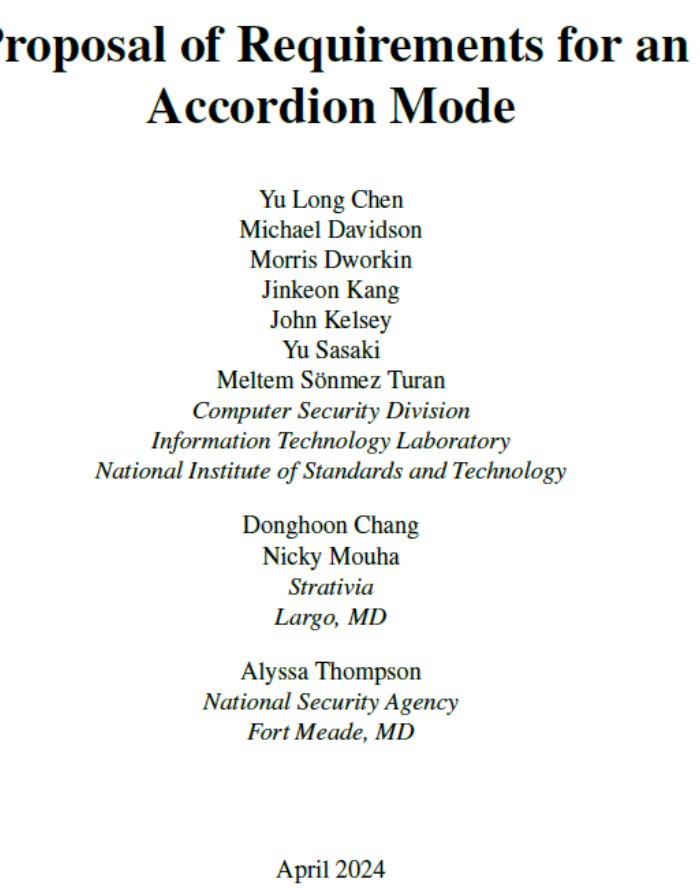
- Wide block cipher (e.g., Rijndael with 256-bit block)
- Keccak-based authenticated encryption
- AES-GCM-SIV, AES-SIV
- Standardizing a fully committing AEAD scheme

Accordion Mode

NIST proposal:

Development of a new AES mode that is a tweakable, variable–input–length strong pseudo-random permutation (VIL-SPRP) with a reduction proof to the security of the underlying block cipher.

Comments due: July 1, 2024



Proposal of Requirements for an Accordion Mode

Yu Long Chen
Michael Davidson
Morris Dworkin
Jinkeon Kang
John Kelsey
Yu Sasaki
Meltem Sönmez Turan
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Donghoon Chang
Nicky Mouha
Strativia
Largo, MD

Alyssa Thompson
National Security Agency
Fort Meade, MD

April 2024

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

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

CONTACT US

Technical inquiries: ciphermodes@nist.gov

For publication reviews: cryptopubreviewboard@nist.gov

Public forum: ciphermodes-forum@list.nist.gov

Website: https://csrc.nist.gov/projects/block-cipher-techniques/bcm