NIST Special Publication 800
NIST SP 800-38Er1 ipd

Recommendation for Block Cipher Modes of Operation

XTS-AES Mode for Confidentiality on Storage Devices

(Initial Public Draft)

Meltem Sonmez Turan
Eric A. Hibbard

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-38Er1.ipd

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

NIST Special Publication 800
NIST SP 800-38Er1 ipd

Recommendation for Block Cipher Modes of Operation

XTS-AES Mode for Confidentiality on Storage Devices

(Initial Public Draft)

Meltem Sonmez Turan [1], Eric A. Hibbard [2]

[1] Computer Security Division, Information Technology Laboratory, NIST
[2] Samsung Semiconductor, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-38Er1.ipd

September 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Technical Series Publications: https://www.nist.gov/nist-research-library/nist-publications

SP 800 Series

The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

References to Other Publications

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications

Non-Endorsement Disclaimer

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the recommendations or requirements in this Information Technology Laboratory (ITL) draft publication). Such recommendations and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

1. assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
2. assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the recommendations or requirements in this ITL draft publication either:
    (a) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    (b) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: SP800-38E-comments@list.nist.gov

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added upon final publication].

The present version is the Initial Public Draft.

Supersedes NIST <Series XXX> (Month Year), DOI:<Insert doi here> [Will be added upon final publication]

Suggested Citation

Meltem Sonmez Turan, Eric A. Hibbard (2026). Recommendation for Block Cipher Modes of Operation: XTS-AES Mode for Confidentiality on Storage Devices. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication 800 (SP) NIST SP 800-38Er1 ipd (Initial Public Draft). DOI:10.6028/NIST.SP.800-38Er1.ipd

Author Names and ORCID Identifiers

Meltem Sonmez Turan (0000-0002-1950-7130); Eric A. Hibbard (0009-0001-8112-1263).

Additional Information

Additional information about this publication, including related content, potential updates, and document history, is available at https://csrc.nist.gov/pubs/sp/800/38/e/r1/ipd.

Public Comments Period: September 3, 2026 – October 16, 2026

Public Comments Contact: SP800-38E-comments@list.nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA)

Abstract

Block cipher modes of operation specify how an **approved** block cipher, such as the Advanced Encryption Standard (AES), is applied to provide cryptographic protection for particular applications, including storage encryption where data is organized in fixed-size units and encrypted without data expansion. Revision 1 of Special Publication (SP) 800-38E approves the XTS-AES mode as specified in IEEE Std. 1619-2025 for protecting the confidentiality of data on block-oriented storage devices. This approval is subject to the applicability statements, conformance requirements, and clarifications in this recommendation. XTS-AES does not provide authentication of the data or its source.

Keywords

Advanced Encryption Standard (AES); block cipher; ciphertext stealing; confidentiality; cryptography; data at rest; encryption; information security; key scope; mode of operation; storage device; tweakable block cipher.

Table of Contents

Acknowledgments

The authors thank Morris Dworkin for authoring the original version of SP 800-38E, which served as the basis for this revision.

Note to the Reviewers

NIST recognizes that IEEE Std. 1619-2025 is maintained and distributed by IEEE, and access to the full technical specification is governed by IEEE's publication policies. To support public review of this draft recommendation, IEEE Std. 1619-2025 will be made publicly available during the public comment period for this publication at https://app.box.com/s/l7v69bw75kit5exqr13vgzhlwf0hg0kh.

This recommendation incorporates IEEE Std. 1619-2025 by reference rather than reproducing the standard. To support public review and implementation, this recommendation summarizes the NIST approval scope, key applicability limitations, conformance requirements, and security considerations for XTS-AES. Implementers seeking to claim conformance with this recommendation are responsible for satisfying the applicable requirements of IEEE Std. 1619-2025 and the additional requirements and clarifications in this recommendation.

1. Introduction

A *mode of operation* specifies how a symmetric-key block cipher is applied to data in order to provide a cryptographic service, such as confidentiality or authentication. The Special Publication (SP) 800-38 series of recommendations [1–6] specifies approved modes of operation for symmetric-key block ciphers. This publication is Part E of that series and focuses on the use of XTS-AES[1] for the confidentiality protection of data on storage devices.

XTS-AES is a mode of operation of the Advanced Encryption Standard (AES) algorithm [7]. It was developed by the IEEE Security in Storage Working Group[2] and was originally specified in IEEE Std. 1619-2007 for the cryptographic protection of data on block-oriented storage devices. SP 800-38E was published in 2010 to approve XTS-AES by reference to IEEE Std. 1619-2007. Revision 1 updates that reference to IEEE Std. 1619-2025 [8].

This recommendation **approves** XTS-AES, as specified in IEEE Std. 1619-2025, subject to the applicability statements, conformance requirements, and clarifications in this recommendation. Revision 1 also clarifies NIST's approval of XTS-AES, including its approved scope of use, conformance requirements, key-scope and data-unit limits, security limitations, and the role of IEEE Std. 1619-2025 as the authoritative technical specification of the mode.

XTS-AES is **approved** only for the confidentiality protection of data on block-oriented storage devices in which data is organized into data units of a fixed length within a key scope. It is not approved as a general-purpose confidentiality mode and is not intended for other applications, such as data in transit, message encryption, key wrapping, or applications that require authenticated encryption.

XTS-AES is based on Rogaway's XEX (XOR Encrypt XOR) tweakable block cipher construction [9], with *ciphertext stealing* added to support data units whose lengths are not integer multiples of the AES block size. The underlying XEX construction applies to sequences of complete 128-bit blocks. In contrast, XTS-AES can be applied to a data unit that consists of one or more complete 128-bit blocks followed by a single, non-empty partial block.

Annex D of IEEE Std. 1619-2025 [8] provides additional discussion of the design choices for XTS-AES, including its resistance to certain forms of ciphertext manipulation and

[1] The acronym XTS stands for XEX Tweakable Block Cipher with Ciphertext Stealing.
[2] The IEEE Security in Storage Working Group operates under the Cybersecurity and Privacy Standards Committee of the Institute of Electrical and Electronics Engineers, Inc. (IEEE).

the implications of those design choices for incorporating XTS-AES into an information system. Prospective implementers should consider this information when determining whether XTS-AES is appropriate for a given threat model.

The remainder of this recommendation is organized as follows.

- Section 2 defines the scope of NIST's approval of XTS-AES and explains the role of IEEE Std. 1619-2025 as the referenced technical specification.
- Section 3 summarizes important terms and concepts.
- Section 4 specifies the conformance requirements, including the data-unit and key-scope limits.
- Section 5 clarifies the ordering convention for the ciphertext-stealing case.

2. Approval, Scope, and Applicability

This recommendation **approves** XTS-AES, as specified in IEEE Std. 1619-2025 [8], for the confidentiality protection of data on block-oriented storage devices. This approval is subject to the applicability statements, conformance requirements, and clarifications in this recommendation.

Algorithmic details are specified in IEEE Std. 1619-2025 and are not repeated in this recommendation, including the XTS-AES encryption and decryption procedures, data-unit processing, underlying keying specifications, and test vectors. For dated references, the edition cited applies. Therefore, this recommendation approves XTS-AES as specified in IEEE Std. 1619-2025, not any later revision or an amendment, unless this recommendation is updated to incorporate that later document.

XTS-AES is intended for storage environments in which data is organized into data units and encrypted without data expansion. The approval in this recommendation does not apply to uses outside of the scope of storage encryption, such as data in transit, message encryption, key wrapping, or applications that require authenticated encryption. XTS-AES provides confidentiality but does not provide authentication or integrity protection; applications that require those protections need additional mechanisms outside of XTS-AES.

3. Terms and Concepts

This section summarizes selected terms and concepts that are especially important for interpreting the approval and conformance requirements in this recommendation. The definitions in IEEE Std. 1619-2025 apply.

Term	Description
ciphertext stealing	A method used by XTS-AES to process a data unit whose length is not an integer multiple of the AES block size without expanding the ciphertext.
data unit	Data within a key scope that is encrypted under XTS-AES. A data unit is at least 128 bits long. Data units within a key scope have equal size and need not correspond exactly to physical or logical blocks on a storage device.
key scope	The data encrypted by a particular key and divided into equal-sized data units to which an adversary might reasonably gain access.
XTS-AES *key*	A 256-bit or 512-bit secret key that is parsed as the concatenation of two AES keys of equal size, denoted as the data encryption key and the tweak key.
tweak value	A 128-bit value that represents the logical position of the data being encrypted or decrypted. The tweak value is also known as the data-unit sequence number.

4. Conformance

An implementation **may** claim conformance with this recommendation if each supported instance of XTS-AES satisfies the applicable requirements of IEEE Std. 1619-2025 [8] and the requirements and clarifications in this recommendation.

XTS-AES instances. An instance of an XTS-AES implementation is defined by the following elements:

1. An XTS-AES key;
2. A single, fixed length for the data units protected by that key; and
3. An implementation of the XTS-AES encryption procedure, the XTS-AES decryption procedure, or both for the specified key and the data-unit length.

Data-unit requirements. The data-unit size **shall** be at least 128 bits. A data unit is divided into 128-bit blocks with at most one partial block. The number of 128-bit blocks in a data unit **shall not** exceed 2^{20}, as specified in IEEE Std. 1619-2025 [8].

Key-scope limits. The total number of 128-bit blocks in a key scope **shall not** exceed 2^{44}. For optimum security, the number of 128-bit blocks in a key scope **should not** exceed 2^{36}.

Supported subsets. An implementation **may** restrict the supported lengths of data units. For example, an implementation may support only data units that consist of complete 128-bit blocks. In that case, the ciphertext-stealing components of the XTS-AES encryption and decryption procedures are unnecessary, and those procedures effectively reduce to the single-block procedures specified in IEEE Std. 1619-2025 [8].

Similarly, an implementation **may** restrict its support to XTS-AES-128, which uses two 128-bit AES keys for a total XTS-AES key length of 256 bits, or to XTS-AES-256, which uses two 256-bit AES keys for a total XTS-AES key length of 512 bits.

The two AES keys, Key_1 and Key_2, used in an XTS-AES key **shall not** be equal, as specified in IEEE Std. 1619-2025 [8]. Implementations **shall** explicitly verify that $Key_1 \neq Key_2$ before the keys are used for XTS-AES encryption or decryption. Although equality is negligibly likely when the two keys are properly generated or established independently, an improper key-generation or key-establishment process may result in equal keys. Equality of Key_1 and Key_2 can expose XTS-AES to the chosen-ciphertext attack identified by Rogaway for the $j = 0$ case of the single-key XEX construction [9].

Restrictions on the supported key lengths or data-unit lengths may affect interoperability with other implementations.

Validation testing. Validation testing for implementations of XTS-AES is conducted within the framework of the Cryptographic Module Validation Program (CMVP), which is a joint effort of NIST and the Communications Security Establishment Canada.

5. Ordering Convention for the Ciphertext Stealing Case

If the length of a data unit for an instance of XTS-AES is not an integral multiple of the AES block size, then the plaintext data unit consists of a sequence of complete blocks $P_0, P_1, \ldots, P_{m-1}$ followed by a single, non-empty partial block P_m, where m is a positive

integer determined by the length of the data unit. In this case, the ciphertext data unit has the same structure: a sequence of complete blocks denoted $C_0, C_1, \ldots, C_{m-1}$ followed by a single, non-empty partial block C_m whose length is the same as the length of P_m.

IEEE Std. 1619-2025 [8] specifies an ordering convention for the final complete ciphertext block and the partial ciphertext block in the ciphertext-stealing case. Some implementations may store these elements in the opposite physical order to follow the order in which the values are generated internally. In particular, C_m is the truncation of a block derived from P_{m-1}, and C_{m-1} is derived from P_m concatenated with the discarded bits from that truncation.

Such physical storage choices do not affect conformance with this recommendation, provided that every external interface presents the ciphertext in the ordering specified by IEEE Std. 1619-2025. In particular, an implementation that stores the final complete block and the partial block in a different physical order needs a mechanism to present them in the standard ordering at its external interfaces so that interoperability is not compromised.

Subclause 5.1 of IEEE Std. 1619-2025 [8] states that an implementation should include documentation describing the mapping between a data unit and the transfer, placement, and composition of data on the storage device, but this mapping is outside of the scope of the standard. This implementation-specific mapping is distinct from the externally visible ordering of the ciphertext specified by IEEE Std. 1619-2025.

References

[1] Dworkin M (2001) Recommendation for Block Cipher Modes of Operation: Methods and Techniques, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A. DOI:10.6028/NIST.SP.800-38A.

[2] Dworkin M (2005) Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38B. DOI:10.6028/NIST.SP.800-38B.

[3] Dworkin M (2004) Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38C. DOI:10.6028/NIST.SP.800-38C.

[4] Dworkin M (2007) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38D. DOI:10.6028/NIST.SP.800-38D.

[5] Dworkin M (2012) Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38F. DOI:10.6028/NIST.SP.800-38F.

[6] Dworkin M (2016) Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38G. DOI:10.6028/NIST.SP.800-38G.

[7] National Institute of Standards and Technology (2001) Announcing the Advanced Encryption Standard (AES) (U.S. Department of Commerce, National Institute of Standards and Technology), Federal Information Processing Standards Publication 197. DOI:10.6028/NIST.FIPS.197

[8] Institute of Electrical and Electronics Engineers (2025) IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. https://standards.ieee.org/ieee/1619/11552/.

[9] Rogaway P (2004) Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. *Advances in Cryptology—ASIACRYPT 2004*, ed Lee PJ (Springer, Berlin, Heidelberg), *Lecture Notes in Computer Science*, Vol. 3329, pp 16–31. DOI:10.1007/978-3-540-30539-2_2