



IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

IEEE Computer Society

Sponsored by the
Storage Systems Standards Committee
and the
Information Assurance Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
18 April 2008

IEEE Std 1619™-2007

IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

Sponsor
**Information Assurance Standards Committee
and the
Storage Systems Standards Committee**
of the
IEEE Computer Society

Approved 5 December 2007

IEEE-SA Standards Board

Abstract: Cryptographic transform and key archival methods for protection of data in sector-level storage devices are specified.

Keywords: data-at-rest security, encryption, key management, security, storage, XTS

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2008 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 18 April 2008. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent and Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-5362-9 STD95754
Print: ISBN 978-0-7381-5363-6 STDPD95754

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied **“AS IS.”**

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE Std 1619, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices.

The purpose of this standard is to describe a method of encryption for data stored in sector-based devices where the threat model includes possible access to stored data by the adversary. The standard specifies the encryption transform and a method for exporting/importing encryption keys for compatibility between different implementations. Encryption of data in transit is not covered by this standard.

This standard defines the XTS-AES tweakable block cipher and its use for encryption of sector-based storage. XTS-AES is a tweakable block cipher that acts on data units of 128 bits or more and uses the AES block cipher as a subroutine. The key material for XTS-AES consists of a data encryption key (used by the AES block cipher) as well as a “tweak key” that is used to incorporate the logical position of the data block into the encryption. XTS-AES is a concrete instantiation of the class of tweakable block ciphers described in Rogaway [B10].^a The XTS-AES addresses threats such as copy-and-paste attack, while allowing parallelization and pipelining in cipher implementations.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at <http://standards.ieee.org>.

^a The numbers in brackets correspond to those of the bibliography in Annex A.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this guide are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

The Security in Storage Working Group operated under the following sponsorship:

Sponsor: John L. Cole
Co-Sponsor: Curtis Anderson

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Security in Storage Working Group had the following officers:

Matthew V. Ball, *Chair*
Eric A. Hibbard, *Vice-chair*
James P. Hughes, *Past chair*
Fabio Maino, *Secretary*

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P1619 Task Group had the following membership:

Serge Plotkin, *Task Group Chair and Technical Editor*

Gideon Avida
Matthew V. Ball
David L. Black
Russel S. Dietz
Robert C. Elliott
Hal Finney
John Goldman
Robert W. Griffin
Cyril Guyot

Shai Halevi
Laszlo Hars
Larry D. Hofer
Walter A. Hubis
James P. Hughes
Glen Jaquette
Curt Kolovson
Robert A. Lockhart
Fabio R. Maino

Charlie Martin
David A. McGrew
Dalit Naor
Landon Curt Noll
Jim Norton
Scott Painter
David B. Sheehy
Robert N. Snively
Douglas L. Whiting

This document was edited by Serge Plotkin (*past vice-chair*), Shai Halevi, and Dalit Naor.

Special thanks to Douglas L. Whiting, Brian Gladman, and Robert C. Elliott.

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Curtis C. Anderson
Danilo Antonelli
Gideon Avida
Matthew V. Ball
Brian A. Berg
Massimo Cardaci
Juan C. Carreon
Keith Chow
John L. Cole
Roger Cummings
Geoffrey Darnton
Russell S. Dietz
Carlo Donati
Robert C. Elliott
Yaacov Fenster
John Goldman

Robert W. Griffin
Randall Groves
Laszlo Hars
Eric A. Hibbard
Werner Hoelzl
Larry D. Hofer
Stuart Holoman
Walter A. Hubis
Raj Jain
Piotr Karocki
Kenneth Lang
Daniel G. Levesque
Robert A. Lockhart
Fabio R. Maino
Edward McCall

Michael Newman
Charles K. Ngethe
Landon Curt Noll
Serge Plotkin
Ulrich Pohl
Jose Puthenkulam
Michael D. Rush
Randall M. Safier
Stephen Schwarm
David B. Sheehy
Robert N. Snively
Thomas Starai
Walter Struppler
John Vergis
Oren Yuen
Paolo Zangheri

When the IEEE-SA Standards Board approved this standard on 5 December 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio
Alex Gelman
William R. Goldbach
Arnold M. Greenspan
Joanna N. Guenin
Julian Forster*
Kenneth S. Hanus
William B. Hopf

Richard H. Hulett
Hermann Koch
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Tom A. Prevost

Narayanan Ramachandran
Greg Ratta
Robby Robson
Anne-Marie Sahazizian
Virginia C. Sulzberger
Malcolm V. Thaden
Richard L. Townsend
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*

Lorraine Patsco
IEEE Standards Program Manager, Document Development

Michael Kipness
IEEE Standards Program Manager, Technical Program Development

CONTENTS

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 Related work	1
2. Normative references	2
3. Definitions, acronyms, and abbreviations	2
3.1 Definitions	2
3.2 Acronyms and abbreviations	2
4. Special terms	2
4.1 Numerical values	2
4.2 Letter symbols	3
4.3 Special definitions	3
5. XTS-AES transform	3
5.1 Data units and tweaks	3
5.2 Multiplication by a primitive element α	4
5.3 XTS-AES encryption procedure	4
5.4 XTS-AES decryption procedure	6
6. Using XTS-AES-128 and XTS-AES-256 for encryption of storage	8
7. Exporting and archiving XTS-AES-128 and XTS-AES-256 keys	9
7.1 Key backup structure	9
7.2 XML format	11
7.3 Encryption of key backup material	13
Annex A (informative) Bibliography	15
Annex B (informative) Test vectors	16
Annex C (informative) Pseudocode for XTS-AES-128 and XTS-AES-256 encryption	25
C.1 Encryption of a data unit with a size that is a multiple of 16 bytes	25
C.2 Encryption of a data unit with a size that is not a multiple of 16 bytes	26
Annex D (informative) Rationale and design choices	27
D.1 Purpose	27
D.2 Transparent encryption	27
D.3 Wide vs. narrow block tweakable encryption	28
D.4 XEX construction	29

D.5 Sector-size that is not a multiple of 128 bits	32
D.6 Miscellaneous	32

IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This standard specifies elements of an architecture for cryptographic protection of data on block-oriented storage devices, describing the methods, algorithms, and modes of data protection to be used.

1.2 Purpose

This standard defines specific elements of an architecture for cryptographically protecting data stored in constant length blocks. Specification of such a mechanism provides an additional and improved tool for implementation of secure and interoperable protection of data residing in storage.

1.3 Related work

The formal definition of the security goal of a tweakable block-cipher can be attributed to Liskov, Rivest, and Wagner [B5]¹, where they also show how tweakable ciphers can be built from standard block ciphers. An earlier work by Schroepel suggested the idea of a tweakable block-cipher, by designing a cipher that natively incorporates a tweak (see Schroepel [B11]).

¹ The numbers in brackets correspond to those of the bibliography in Annex A.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

NIST FIPS-197, Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard (AES).²

REC-xml, W3C Extensible Markup Language (XML) 1.0 (Fourth Edition).³

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition* [B4] should be referenced for terms not defined in this clause.

3.1.1 key scope: Data encrypted by a particular key, divided into equal-sized data units. The key scope is identified by three non-negative integers: tweak value corresponding to the first data unit, the data unit size, and the length of the data.

NOTE—See 4.3.1.⁴

3.1.2 tweak value: The 128-bit value used to represent the logical position of the data being encrypted or decrypted with XTS-AES.

3.2 Acronyms and abbreviations

AES	advanced encryption standard
Base64	encoding according to IETF RFC 3548 [B12]
DTD	document type definition
FIPS	Federal Information Processing Standard
GF	Galois field (see Menezes et. al. [B6])
LBA	logical block address
XML	extensible markup language
XTS	XEX encryption mode with tweak and ciphertext stealing

4. Special terms

4.1 Numerical values

Decimal and binary numbers are used within this document. For clarity, decimal numbers are generally used to represent counts and binary numbers are used to describe bit patterns.

² FIPS publications are available from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22661, USA. FIPS-197 is also available on-line from <http://csrc.nist.gov/publications/fips/index>.

³ Available at <http://www.w3.org/TR/REC-xml/>

⁴ Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

Decimal numbers are represented in their usual 0, 1, 2, ... format. Binary numbers are represented by a string of one or more bits followed by the subscript 2. Thus the decimal number 26 may also be represented as 00011010₂. Hexadecimal numbers are represented by a string of one or more hexadecimal characters followed by a subscript 16.

4.2 Letter symbols

The following symbols are used in equations and figures:

$\oplus$	Bit-wise exclusive-OR operation
$\otimes$	Modular multiplication of two polynomials over the binary field GF(2), modulo $x^{128} + x^7 + x^2 + x + 1$, where GF stands for Galois Field (see Menezes et. al. [B6])
α	A primitive element of GF(2 ¹²⁸) that corresponds to polynomial x (i.e., 0000...010 ₂), where GF stands for Galois Field (see Menezes et. al. [B6])
$\bullet$	Assignment of a value to a variable
	Concatenation (e.g., if K1 = 001 ₂ and K2 = 101010 ₂ , then K1 K2 = 001101010 ₂)
//	Start of a comment. Comment ends at end of line
$\lfloor x \rfloor$	Floor of x (e.g., $\lfloor 7/3 \rfloor = 2$)

4.3 Special definitions

4.3.1 Data unit: Within IEEE Std 1619, 128 or more bits of data within a key scope. The first data unit in a key scope starts with the first bit of the key scope; each subsequent data unit starts with the bit after the end of the previous data unit. Data units within a key scope are of equal sizes. A data unit does not necessarily correspond to a physical or logical block on the storage device.

5. XTS-AES transform

5.1 Data units and tweaks

This standard applies to encryption of a data stream divided into consecutive equal-size data units, where the data stream refers to the information that has to be encrypted and stored on the storage device. Information that is not to be encrypted is considered to be outside of the data stream.

The data unit size shall be at least 128 bits. Data unit should be divided into 128-bit blocks. Last part of the data unit might be shorter than 128 bits. The number of 128-bit blocks in the data unit shall not exceed $2^{128} - 2$. The number of 128-bit blocks should not exceed 2^{20} . Each data unit is assigned a tweak value that is a non-negative integer. The tweak values are assigned consecutively, starting from an arbitrary non-negative integer. When encrypting a tweak value using AES, the tweak is first converted into a little-endian byte array. For example, tweak value 123456789a₁₆ corresponds to byte array 9a₁₆, 78₁₆, 56₁₆, 34₁₆, 12₁₆.

The mapping between the data unit and the transfer, placement, and composition of data on the storage device is beyond the scope of this standard. Devices compliant with this standard should include