INTERNATIONAL STANDARD

ISO/IEC 10116

Fourth edition
2017-07

AMENDMENT 1
2021-02

Information technology — Security techniques — Modes of operation for an n-bit block cipher

AMENDMENT 1: CTR-ACPKM mode of operation

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n bits

AMENDEMENT 1

Reference number
ISO/IEC 10116:2017/Amd.1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Information technology — Security techniques — Modes of operation for an n-bit block cipher

AMENDMENT 1: CTR-ACPKM mode of operation

Introduction

Delete the NOTE and replace the second paragraph with the following:

This document specifies the following modes of operation:

a) electronic codebook (ECB);

b) cipher block chaining (CBC);

c) cipher feedback (CFB);

d) output feedback (OFB);

e) counter (CTR);

f) counter advanced cryptographic prolongation of key material (CTR-ACPKM).

Scope

Replace the first sentence of the first paragraph with the following:

This document establishes the modes of operation for applications of an *n*-bit block cipher (e.g. protection of data during transmission or in storage).

Delete NOTE 3 and NOTE 4.

Clause 3, Terms and definitions

Replace the terminological entry with the following:

3.3
counter
bit array of length *n* bits (where *n* is the block size of the underlying block cipher) which is used in CTR mode and CTR-ACPKM mode

Add new entries 3.13 to 3.15 as follows:

3.13
key lifetime
maximum amount of data that could be processed using this key by the particular mode of operation without loss of some proven security property

3.14
section
part of plaintext that is processed with one key before this key is transformed

3.15
section key
key used to process one section

4.1

Add the following rows at the end of the table:

c	number of bits in a counter which can be modified during incrementing in the CTR-ACPKM mode
J	number of constants in the ACPKM transformation
$K^{(z)}$	section key
len	length of the plaintext (in bits)
N	section size (the number of bits that are processed with one section key before this key is transformed)
s	number of sections
z	iteration for sections

4.2

Replace the third row with the following:

$a(t)$	t-bit string where the value 'a' (0 or 1) is assigned to every bit

Add the following row at the end of the table:

$\lceil a \rceil$	smallest integer that is greater than or equal to a

Clause 5

Add the following sentence after the fourth sentence of the second paragraph:

> For the counter advanced cryptographic prolongation of key material (CTR-ACPKM) mode of operation (see Clause 11), three parameters c, j and N need to be selected.

Replace the first sentence of the fourth paragraph with the following:

> For the ECB, CBC, CFB, OFB and CTR modes of operation, the encrypter and all potential decrypters shall agree on a padding method, unless messages to be encrypted are always a multiple of m bits ($m = n$ for ECB and CBC modes, $m = j$ for CFB, OFB and CTR modes) in length or unless the mode does not require padding.

Add the following sentence at the end of the fourth paragraph:

> For the CTR-ACPKM mode of operation, padding is not used by default and the bit length of the plaintext need not be a multiple of j bits. If any padding is applied by the application that invokes the encryption, then the padding method shall be known to the application that invokes the decryption.