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)

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.

Add the following paragraphs at the end of the clause:

> The modes of operation specified in this document have been assigned object identifiers in accordance with ISO/IEC 9834 (all parts). Annex A lists the object identifiers which shall be used to identify the modes of operation specified in this document.
>
> Annex B contains comments on the properties of each mode and important security guidance.
>
> Annex C presents figures describing the modes of operation. Annex D provides numerical examples of the modes of operation.

7.2

Replace the last sentence with the following:

> This procedure is shown on the Figure C.1 for $m = 1$ and on the left side of Figure C.2 for $m > 1$.

7.3

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

> This procedure is shown on the Figure C.1 for $m = 1$ and on the right side of Figure C.2 for $m > 1$.

Clause 11

Add new Clause 11 as follows:

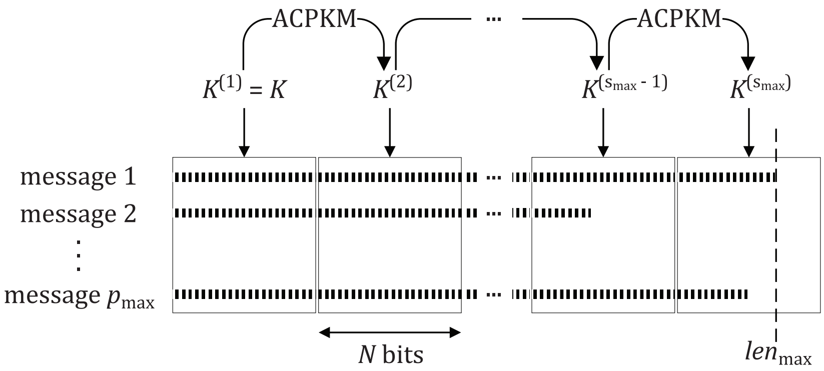
11 Counter advanced cryptographic prolongation of key material (CTR-ACPKM) mode

11.1 General

The CTR-ACPKM mode employs an approach to increase the key lifetime by using a transformation of a data processing key (section key) during the processing of each message. Each message is processed starting with the same first section key and each section key is updated after processing one section which consists of N bits.

NOTE CTR-ACPKM mode is the same as CTR mode except that the key is transformed during processing of the mode.

The main idea behind the CTR-ACPKM mode is presented in Figure 1.



Key

p_{max} maximum number of messages encrypted under one initial key K

len_{max} maximum length of message (in bits)

s_{max} $\lceil len_{max} / N \rceil$

Figure 1 — Basic principles of message processing in the CTR-ACPKM mode

During the processing of the plaintext message P of length len (in bits) in the CTR-ACPKM encryption mode the message is divided into $s = \lceil len_{max} / N \rceil$ sections (denoted by P^1, ..., P^s, where P^z has an N-bit length for $1 \le z \le s-1$ and the length of the last section P^s can be less than or equal to N bits). The first section of each message is processed with the section key $K^{(1)}$, which is equal to the initial key K. To process the (z+1)-th section of each message the section key $K^{(z+1)}$ is calculated using the ACPKM transformation defined in 11.5.

11.2 Preliminaries

For the CTR-ACPKM mode the block size n of the chosen block cipher shall be a multiple of 8.

Three parameters define the CTR-ACPKM mode of operation:

— the size of the plaintext variable j, where $1 \le j \le n$ and j is a multiple of 8;

— the section size in bits, N, where N is a multiple of j;

— the number of bits in a counter to be incremented, c, where $0 < c < n$ and c is a multiple of 8.

The variables employed by the CTR-ACPKM mode of operation when being used for encryption are:

a) the input variables:

1) a plaintext message P of length len, which can be represented as:

— a concatenation of q plaintext variables $P_1 | P_2 | \dots | P_q$, where P_1, P_2, ..., P_{q-1} are j-bit strings and P_q contains less than or equal to j bits;

— a concatenation of s section variables $P^1 | P^2 | \dots | P^s$, where P^1, P^2, ..., P^{s-1} are N-bit strings and P^s contains less than or equal to N bits;

2) an initial key K;

3) a starting variable SV of $n-c$ bits. See Annex B for security guidance on the value of SV;

b) the intermediate results:

1) a sequence of s section keys $K^{(1)}$, $K^{(2)}$, … , $K^{(s)}$, each of k bits;

2) a sequence of q block cipher input blocks CTR_1, CTR_2, ..., CTR_q, each of n bits;

3) a sequence of q block cipher output blocks Y_1, Y_2, ..., Y_q, each of n bits;

4) a sequence of q variables E_1, E_2, ..., E_q, each of j bits;

c) the output variable: an encrypted message C of length *len*, which can be represented as a concatenation of q ciphertext variables $C_1|C_2|...|C_q$, where C_1, C_2, ..., C_{q-1} are j-bit strings and C_q contains less than or equal to j bits.

Using the CTR-ACPKM mode it is possible to avoid ciphertext expansion by truncating the variable E_q to the length of the final plaintext/ciphertext variable. The bit length of the plaintext message P need not be a multiple of j (the bit length of the last plaintext/ciphertext variable P_q/C_q can be less than or equal to j).

The following limitations should be observed when using the CTR-ACPKM mode (see Annex B for a detailed explanation of these limitations):

— the length *len* of every message should be less than or equal to $j \cdot 2^{c-1}$;

— the number of messages encrypted under one initial key K should be less than or equal to 2^{n-c}.

11.3 Encryption

The section keys are generated from the initial key K using the *ACPKM* key transformation defined in 11.5.

a) The first section key $K^{(1)}$ is equal to the initial key K : $K^{(1)} = K$.

b) For z = 2, ..., s, where $s = \lceil len / N \rceil$, the section key $K^{(z)}$ is generated as follows:

$$K^{(z)} = ACPKM\left(K^{(z-1)}\right).$$

The counter CTR is set using the starting variable padded with c zeros:

$$CTR_1 = SV|0(c).$$

The operation of encrypting each plaintext variable P_i employs the following four steps.

a) $Y_i = eK^{(z)}(CTR_i)$, where $z = \lceil i \cdot j / N \rceil$ (use of block cipher);

b) $E_i = j \sim Y_i$ (selection of leftmost j bits of Y_i);

c) $C_i = P_i \oplus E_i$ (generation of ciphertext variable);

d) $CTR_{i+1} = (CTR_i + 1) \bmod 2^n$ (generation of the next counter value CTR).

These steps are repeated for i = 1, 2, ..., q, ending with step c) on the last cycle. The procedure is shown in Figure C.6.

The counter value CTR_i is encrypted under the corresponding section key $K^{(z)}$ to give an output block Y_i and the leftmost j bits of this output block Y_i are used to encrypt the input value. The counter then increases by one (modulo 2^n) to produce a new counter value.

11.4 Decryption

The variables employed for decryption are the same as those employed for encryption.

The section keys are generated from the initial key K using the *ACPKM* key transformation defined in 11.5.

a) The first section key $K^{(1)}$ is equal to the initial key K: $K^{(1)} = K$.

b) For $z = 2, ..., s$, where $s = \lceil len / N \rceil$, the section key $K^{(z)}$ is generated as follows:

$$K^{(z)} = ACPKM\left(K^{(z-1)}\right).$$

The counter CTR is set using the starting variable padded with c zeros:

$$CTR_1 = SV | 0(c).$$

The operation of decrypting each ciphertext variable C_i employs the following four steps.

a) $Y_i = eK^{(z)}(CTR_i)$, where $z = \lceil i \cdot j / N \rceil$ (use of block cipher);

b) $E_i = j \sim Y_i$ (selection of leftmost j bits of Y_i);

c) $P_i = C_i \oplus E_i$ (generation of plaintext variable);

d) $CTR_{i+1} = (CTR_i + 1) \bmod 2^n$ (generation of the next counter value CTR).

These steps are repeated for $i = 1, 2, ..., q$, ending with step (c) on the last cycle. The procedure is shown in Figure C.6.

The counter value CTR_i is encrypted under the corresponding section key $K^{(z)}$ to give an output block Y_i and the leftmost j bits of this output block Y_i are used to decrypt the input value. The counter then increases by one (modulo 2^n) to produce a new counter value.

11.5 ACPKM transformation

The $ACPKM$ function takes as input the k-bit key $K^{(z)}$ and outputs the k-bit key $K^{(z+1)}$ calculated as follows:

$$K^{(z+1)} = ACPKM\left(K^{(z)}\right) = k \sim \left(eK^{(z)}(D_1) | \ldots | eK^{(z)}(D_J)\right),$$

where $J = \lceil k / n \rceil$, and $D_1, D_2, ..., D_J$ are n-bit strings calculated as follows:

$$D_1 | D_2 | \ldots | D_J = (J \cdot n) \sim D,$$

where D is the 1 024-bit constant that is defined as follows (D is presented in hexadecimal notation, where two consecutive hexadecimal digits correspond exactly to one byte and each 8 bytes are separated by a space for better visibility):

```
8081828384858687 88898a8b8c8d8e8f 9091929394959697 98999a9b9c9d9e9f a0a1a2a3a4a5a6a7
a8a9aaabacadaeaf b0b1b2b3b4b5b6b7 b8b9babbbcbdbebf c0c1c2c3c4c5c6c7 c8c9cacbcccdcecf
d0d1d2d3d4d5d6d7 d8d9dadbdcdddedf e0e1e2e3e4e5e6e7 e8e9eaebecedeeef f0f1f2f3f4f5f6f7
f8f9fafbfcfdfeff
```

Annex A

Change

```
id-mode-cbc_cs1 OID ::= { id-mode cbc_cs1(6) }
id-mode-cbc_cs2 OID ::= { id-mode cbc_cs2(7) }
id-mode-cbc_cs3 OID ::= { id-mode cbc_cs3(8) }
```

to

```
id-mode-cbc-cs1 OID ::= { id-mode cbc-cs1(6) }
id-mode-cbc-cs2 OID ::= { id-mode cbc-cs2(7) }
id-mode-cbc-cs3 OID ::= { id-mode cbc-cs3(8) }
id-mode-ctr-acpkm OID ::= { id-mode ctr-acpkm(9) }
```