INTERNATIONAL STANDARD

ISO/IEC 29192-6

First edition
2019-09

Information technology — Lightweight cryptography —

Part 6: Message authentication codes (MACs)

Technologies de l'information — Cryptographie pour environnements contraints —

Partie 6: Codes d'authentification de message (MACs)

Reference number
ISO/IEC 29192-6:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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).

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 http://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.

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

A list of all parts in the ISO/IEC 29192 series can be found on the ISO website.

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.

Introduction

In an IT environment, it is often required that one can verify that electronic data has not been altered in an unauthorized manner and that one can provide assurance that a message has been originated by an entity in possession of the secret key. A MAC (Message Authentication Code) algorithm is a commonly used data integrity mechanism that can satisfy these requirements.

It is possible to take the first approach to realize a lightweight MAC by using the specified MAC algorithm in conjunction with a block cipher that can be chosen from ISO/IEC 29192-2 or ISO/IEC 18033-3, and in conjunction with a hash-function that can be chosen from ISO/IEC 29192-5. It is also possible to take the second approach to realize a lightweight MAC using a dedicated function. Examples of both approaches are specified in this document.

Information technology — Lightweight cryptography —

Part 6:
Message authentication codes (MACs)

1 Scope

This document specifies MAC algorithms suitable for applications requiring lightweight cryptographic mechanisms. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key.

The following MAC algorithms are specified in this document:

a) LightMAC;

b) Tsudik's keymode;

c) Chaskey-12.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 29192-2, *Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers*

ISO/IEC 29192-5, *Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18033-3 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
block cipher key
key that controls the operation of a block cipher

[SOURCE: ISO/IEC 9797-1:2011, 3.2]

3.2
encryption
reversible operation by a cryptographic algorithm converting data into ciphertext so as to hide the information content of the data

[SOURCE: ISO/IEC 9797-1:2011, 3.6]

3.3
hash-function
function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 10118-1:2016, 3.4]

3.4
key
sequence of symbols that controls the operation of a cryptographic transformation

Note 1 to entry: Examples are encryption, decryption, cryptographic check function computation, signature, generation, or signature verification.

[SOURCE: ISO/IEC 9797-1:2011, 3.7]

3.5
Message Authentication Code
MAC
string of bits which is the output of a MAC algorithm

[SOURCE: ISO/IEC 9797-1:2011, 3.9]

3.6
MAC algorithm
algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

— for any key and any input string, the function can be computed efficiently;

— for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of a set of input strings and corresponding function values, where the value of the ith input string might have been chosen after observing the value of the first i - 1 function values (for integers $i > 1$)

[SOURCE: ISO/IEC 9797-1:2011, 3.10]

3.7
word
string of 32 bits used in Chaskey-12 MAC algorithm

4 Symbols and abbreviated terms

$a \leftarrow b$	set variable a to the value of b
$E(K, P)$	encryption of the plaintext P with the block cipher E using the key K
h	hash-function

IV	t-bit initializing value
I2BS(x, g)	function that takes as input a non-negative integer x and outputs a bit string of length g corresponding to its binary representation
K_i	block cipher key taken by the underlying block cipher used in LightMAC (i = 1, 2)
m	message string to be input to the MAC algorithm
m'	message string after the padding has been applied
m_i'	i th n-bit block of the padded-message string m'
$m'_i{}^{(n-s)}$	i th $(n-s)$-bit block of the padded-message string m' for $i < l$ where $m'_1{}^{(n-s)}\|\|m'_2{}^{(n-s)}\|\|...\|\|m'_\ell = m'$
s	counter size
t	length of the MAC in bits
v_i	32-bit words used to store the results of intermediate computations
$X\|_j$	j-bit unsigned integer obtained from the u-bit unsigned integer X by taking the j least significant bits of X ($1 \le j \le u$)
X<<1	operation of left shift by one bit, i.e. if X is a word then X << 1 denotes the word obtained by left-shifting the contents of X by one position
X <<< n	operation of 'circular left shift' by n bit positions, i.e. if X is a word and n is a non-negative integer then X<<<n denotes the word obtained by left-shifting the contents of X by n positions in a cyclic fashion
0^s	string consisting of s zero-bits
$\oplus$	bitwise exclusive-OR operation
$\boxplus$	addition modulo 2^{32}
$\|X\|$	the length of bit string X in bits
$\|\|$	concatenation of bit strings
$+_w$	addition modulo 2^w operation, where w is the number of bits in a word; i.e. if A and B are w–bit words, then $A +_w B$ is the word obtained by treating A and B as the binary representations of integers and computing their sum modulo 2^w, where the result is constrained to lie between 0 and $2^w - 1$ inclusive

5 Lightweight MACs based on block ciphers

5.1 General

This clause specifies a lightweight MAC algorithm that uses a secret key and an n-bit block cipher to calculate a t-bit MAC.

Annex A defines the object identifier which shall be used to identify the algorithm specified in Clause 5. Annex B provides numerical examples for the MAC algorithms in hexadecimal notation. Annex C gives the lightweight properties of the MAC algorithms described in this document.

5.2 LightMAC

5.2.1 General

LightMAC is a MAC algorithm that shall be used with any block cipher from ISO/IEC 29192-2 or ISO/IEC 18033-3. Users who wish to employ LightMAC[6] shall select:

— an n-bit block cipher E from ISO/IEC 29192-2 or ISO/IEC 18033-3;

— a length t in bits of the MAC;

— a counter size s, i.e. the number of bits allocated to represent the counter value, where $0 \leq s < n$.

The above parameters shall remain constant while using LightMAC under a given key. Different parameter sets should not be used under the same key.

NOTE 1 If any of the parameters above are modified while using a key, then no security can be guaranteed.

NOTE 2 Numerical examples, including for the cases s = 8 or 32 and t = 64, are listed in B.2.

LightMAC takes as input two independently generated block cipher keys K_1 and K_2, and a message M of length at most $2^s(n-s)$ bits. LightMAC produces an output of length t bits. LightMAC requires the following steps: padding, application of the block cipher, and truncation.

5.2.2 Step 1 (padding)

Let m be the message input to LightMAC, and $d = |m| \bmod (n-s)$. Right-pad m with a single '1' bit, followed by n-d-1 '0' bits. The result is denoted by m'.

5.2.3 Step 2 (application of the block cipher)

m' shall be split into strings $m'_1, m'_2, \ldots, m'_\ell$, where $m'_1{}^{(n-s)}, m'_2{}^{(n-s)}, \ldots, m'_{\ell-1}{}^{(n-s)}$ are n-s bit strings, m'_ℓ is an n bit string, and $m'_1{}^{(n-s)} || m'_2{}^{(n-s)} || \ldots || m'_\ell = m'$. The string S is computed using the following procedure.

$V \leftarrow 0^n$

For i = 1 to ℓ-1:

$V \leftarrow E(K_1, \text{I2BS}(i, s) || m'_i) \oplus V$

$V \leftarrow m_\ell' \oplus V$

$S \leftarrow E(K_2, V)$

Refer to Annex D for the specification of I2BS.

5.2.4 Step 3 (truncation)

The MAC of t bits is derived by taking the least significant t bits of the string S, i.e.:

$\text{MAC} \leftarrow S|_t$

6 Lightweight MACs based on hash-functions

6.1 General

This clause specifies a lightweight MAC algorithm that uses a lightweight hash-function to compute a MAC.

Annex A defines the object identifier which shall be used to identify the algorithm specified in Clause 6. Annex B provides numerical examples for the MAC algorithms in hexadecimal notation. Annex C gives the lightweight properties of the MAC algorithms described in this document.

6.2 Tsudik's keymode

6.2.1 Requirements

Tsudik's keymode is a MAC algorithm that uses a hash-function. In order to use Tsudik's keymode[1], a lightweight hash-function h shall be selected and agreed. The hash-function shall be chosen from amongst the lightweight hash-functions specified in ISO/IEC 29192-5:2016. An entity generating a MAC shall be equipped with a secret key K, which shall also be made available to all parties needing to verify the MAC.

NOTE 1 Tsudik's keymode is classified as lightweight because the number of calls to the underlying hash-function is typically smaller than generic-purpose hash-function-based MACs such as HMAC, as specified in ISO/IEC 9797-2.

NOTE 2 The reason why the underlying hash-function must be chosen from amongst those specified in ISO/IEC 29192-5 is described in Annex C.

NOTE 3 In the selection of the underlying hash-function used in Tsudik's keymode, it is up to the user to check its security against length extension attacks.

6.2.2 MAC calculation

To compute a MAC over the message m using the Tsudik's keymode, the following operation is performed:

$S \leftarrow h\,(K||m)$.

The MAC of t bits is derived by taking the least significant t bits of the string S, i.e.:

$\text{MAC} \leftarrow S|_t$.

7 Lightweight dedicated MACs

7.1 General

This clause specifies a lightweight dedicated MAC algorithm.

Annex A defines the object identifier which shall be used to identify the algorithm specified in Clause 7. Annex B provides numerical examples for the MAC algorithms in hexadecimal notation. Annex C gives the lightweight properties of the MAC algorithms described in this document.

7.2 Chaskey-12

7.2.1 General

Chaskey-12[8] is a lightweight MAC algorithm that processes an arbitrary-length message m using a key K of length 128 bits. It outputs a MAC of 128 bits or less.

NOTE 1 In the original proposal for the Chaskey algorithm[7], the number of rounds was set to 8, and the algorithm is referred to as Chaskey-8. Because of concerns that 8 rounds are insufficient to guarantee the required level of security, the scheme specified here has 12 rounds, and is thus referred to as Chaskey-12[8].