INTERNATIONAL STANDARD

ISO/IEC 29192-8

First edition
2022-09

Information security — Lightweight cryptography —

Part 8: Authenticated encryption

Sécurité de l'information — Cryptographie pour environnements contraints —

Partie 8: Cryptage authentifié

Reference number
ISO/IEC 29192-8:2022(E)

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 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 https://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 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 and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document specifies authenticated encryption tailored for implementation in constrained environments. Data transmitted from one party to another is often vulnerable against various attacks such as eavesdropping or malicious alterations. Similarly, data at rest usually requires protection.

Encryption mechanisms as specified in the ISO/IEC 18033 series and ISO/IEC 10116 provide solutions against eavesdropping. Integrity protection is usually guaranteed with a message authentication code (MAC) algorithm, such as those defined in the ISO/IEC 9797 series. In addition, ISO/IEC 19772 describes several authenticated encryption mechanisms, that is to say mechanisms that efficiently combine the encryption and MAC operations.

Nonetheless, some applications including radiofrequency identification (RFID) tags, smart cards, secure batteries, health-care systems and sensor networks, encounter several constraints. Chip area, energy consumption, execution time, program code, RAM size and communication bandwidth are typically critical for the applications listed above. The ISO/IEC 29192 series specifies lightweight cryptography suitable for these constrained environments. ISO/IEC 29192-2 and ISO/IEC 29192-3 respectively define lightweight block ciphers and stream ciphers. Both can be used to provide confidentiality. Regarding protection against alteration, lightweight MAC algorithms are defined in ISO/IEC 29192-6.

In this document, lightweight authenticated encryption mechanisms are defined. Similar to ISO/IEC 19772, they provide confidentiality, integrity and optionally data origin authentication. They differ from those specified in the aforementioned document, in that they have been specifically designed for constrained environments.

This document specifies a unique method. In the future, other methods may be added to this document, including lightweight authenticated encryption with additional data (AEAD) methods, based either on block ciphers or stream ciphers.

Information security — Lightweight cryptography —

Part 8:
Authenticated encryption

1 Scope

This document specifies one method for authenticated encryption suitable for applications requiring lightweight cryptographic mechanisms.

This method processes a data string with the following security objectives:

a) data confidentiality, i.e. protection against unauthorized disclosure of data,

b) data integrity, i.e. protection that enables the recipient of data to verify that it has not been modified.

Optionally, this method can provide data origin authentication, i.e. protection that enables the recipient of data to verify the identity of the data originator.

The method specified in this document is based on a lightweight stream cipher, and requires the parties of the protected data to share a secret key for this algorithm. Key management is outside the scope of this document.

NOTE Key management techniques are defined in the ISO/IEC 11770 series.

2 Normative references

There are no normative references for this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and optionally data origin authentication

[SOURCE: ISO/IEC 19772:2020, 3.2, modified — The definition was slightly modified to make the data origin authentication optional.]

3.2
authenticated encryption mechanism
cryptographic technique used to protect the confidentiality, guarantee the integrity of data and optionally the data origin and which consists of two component processes: an *encryption* (3.6) algorithm and a *decryption* (3.5) algorithm

[SOURCE: ISO/IEC 19772:2020, 3.3, modified — The definition was slightly modified to make the data origin authentication optional.]

3.3
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 18033-1:2021, 3.7]

3.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO/IEC 9797-1:2011, 3.4]

3.5
decryption
reversal of a corresponding *encryption* (3.6)

[SOURCE: ISO/IEC 9797-1:2011, 3.5]

3.6
encryption
reversible operation by a cryptographic algorithm converting data into *ciphertext* (3.3) so as to hide the information content of the data

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

3.7
initialization value
value used in defining the starting point of an *encryption* (3.6) process

[SOURCE: ISO/IEC 18033-4:2011, 3.7]

3.8
key
sequence of symbols that controls the operation of a cryptographic transformation

[SOURCE: ISO/IEC 9797-1:2011, 3.7, modified — Note was removed.]

3.9
keystream function
function that takes as input, the current *state* (3.17) of the *keystream generator* (3.10) and (optionally) part of the previously generated *ciphertext* (3.3), and gives as output the next part of the keystream

[SOURCE: ISO/IEC 18033-4:2011, 3.9]

3.10
keystream generator
state-based process (i.e. as a finite state machine) that takes as input, a *key* (3.8), an *initialization value* (3.7), and if necessary the *ciphertext* (3.3), and gives as output a keystream (i.e. a sequence of bits or blocks of bits) of arbitrary length

[SOURCE: ISO/IEC 18033-4:2011, 3.10, modified —"initialization vector" changed to "initialization value".]

3.11
message authentication code
MAC
string of bits which is the output of a *MAC algorithm* (3.12)

[SOURCE: ISO/IEC 9797-1:2011, 3.9, modified — Note was removed.]

3.12
message authentication code algorithm
MAC algorithm
algorithm for computing a function which maps strings of bits and a *secret key* (3.16) 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, modified — Notes were removed]

3.13
next-state function
function that takes as input, the current *state* (3.17) of the *keystream generator* (3.10) and (optionally) part of the previously generated *ciphertext* (3.3), and gives as output a new *state* (3.17) for the *keystream generator* (3.10)

[SOURCE: ISO/IEC 18033-4:2011, 3.12]

3.14
plaintext
cleartext
unencrypted information

[SOURCE: ISO/IEC 18033-1:2021, 3.20]

3.15
pre-output stream
pseudo-random bits, which are used for the *encryption* (3.6) and the *decryption* (3.5) of the message, and the generation of the *message authentication code* (3.11)

3.16
secret key
key (3.8) used with symmetric cryptographic techniques by a specified set of entities

[SOURCE: ISO/IEC 18033-1:2021, 3.25]

3.17
state
internal state of *a keystream generator* (3.10)

[SOURCE: ISO/IEC 29192-3:2012, 3.12]

4 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

ACCU Dedicated accumulator register for the MAC (t bits).

AM Authenticated message, the concatenation of the ciphertext C and the MAC. $AM = C \,||\, MAC$.

AND Bitwise logical AND operation.

$AUTH^{(i)}$ Dedicated register for the MAC computation.

a_i Variable forming part of the internal state of a keystream generator.

b_i Variable forming part of the internal state of a keystream generator.

C Ciphertext.

C_i Ciphertext bit.

Fmac Function which finalizes the MAC computation.

Imac Function which initializes the MAC registers.

Init Function which generates the initial internal state of a keystream generator.

IV Initialization value.

K Key.

l Length of a plaintext or ciphertext block (in bits).

Len Function that returns the number of bits in a string.

LFSR Linear feedback shift register.

MAC Message authentication code. MAC is a t-bit string.

M_i Message bit.

n Length of the authenticated message (AM) (in bits).

Next Next-state function of a keystream generator.

NLFSR Nonlinear feedback shift register.

OR Bitwise logical OR operation.

P Plaintext.

P_i Plaintext bit.

Prt Function that generates a pre-output of the stream cipher.

r_i Variable forming part of the internal state of a keystream generator.

SHIFT Dedicated shift register for the MAC (t bits).

s_i Variable forming part of the internal state of a keystream generator.

Strm Keystream function of a keystream generator.

$S^{(i)}$ Internal state of keystream generator.

t MAC length (in bits).

Upmac Function which updates the MAC registers.

Y Pre-output stream.

$Y^{(i)}$ Pre-output bit.

Z Keystream.

$Z^{(i)}$ Keystream bit.

0^i Block of i zero bits.

1^i Block of i one bits.

$\oplus$ Bitwise XOR (eXclusive OR) operation.

$||$ Concatenation of strings, i.e. if A and B are blocks of data, then $A||B$ is the block obtained concatenating A and B in the order specified.

$X|_s$ Left-truncation of the block of bits X: if X has a bit-length greater than or equal to s, then $X|_s$ is the s-bit block consisting of the left-most s bits of X.

$X|^s$ Right-truncation of the block of bits X: if X has a bit-length greater than or equal to s, then $X|^s$ is the s-bit block consisting of the right-most s bits of X.

5 Grain-128A

5.1 Introduction to Grain-128A

Grain-128A is a synchronous stream cipher with an add-on module that generates a message authentication code (MAC).

It is composed of two sub-modules that work conjointly:

a) a stream cipher module that generates the key stream for the encryption/decryption of the message;

b) a MAC module that constitutes the MAC algorithm.

Grain-128A has a 128-bit long key, K, and a 96-bit initialization value, IV. It generates a t-bit MAC.

As a precondition, the recipients will have received K and IV in a secure way as pre-shared parameters.

For this mechanism, t shall be at least equal to 32 and the MAC shall apply to the entire plaintext.

After the initialization of the system with the K and the IV, the cipher generates a pre-output stream. This pre-output stream is split into two parts:

a) the even bits compose the keystream to encrypt/decrypt the message;

b) the odd bits are used to generate the MAC.

NOTE 1 Grain-128A document [12] defines two modes of operation: with or without a MAC. The MAC is disabled when $IV_0 = 0$ and conversely enabled when $IV_0 = 1$. This document only specifies the authenticated mode, i.e. the MAC is always supported. Accordingly, the value of IV_0 is fixed to '1'.

As a synchronous keystream generator, Grain-128A follows the general models of stream ciphers defined in ISO/IEC 18033-4, with supplementary functions to take the MAC generation into consideration.

Grain-128A finite-state machine is defined by:

a) an initialization function, **Init**, which takes as input a key, K, and an initialization value, IV, and outputs an initial state $S^{(-2*t)}$ for the keystream generator;