



BSI Standards Publication

Information technology — Security techniques — Lightweight cryptography

Part 1: General

National foreword

This British Standard is the UK implementation of ISO/IEC 29192-1:2012+A1:2025. It supersedes BS ISO/IEC 29192-1:2012, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 27377 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2012.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2025	Implementation of ISO/IEC amendment 1:2025

**Information technology — Security
techniques — Lightweight
cryptography —**

**Part 1:
General**

*Technologies de l'information — Techniques de sécurité —
Cryptographie pour environnements contraints —*

Partie 1: Généralités



Reference number
ISO/IEC 29192-1:2012(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2012



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents		Page
Foreword		iv
Introduction.....		v
1	Scope	1
2	Terms and definitions	1
3	Categories of constraints for lightweight cryptography	2
3.1	Chip area	2
3.2	Energy consumption.....	2
3.3	Program code size and RAM size	2
3.4	Communication bandwidth	2
3.5	Execution time	3
4	Requirements.....	3
4.1	Security requirements.....	3
4.2	Classification requirements	3
4.3	Implementation requirements	4
5	Lightweight cryptographic mechanisms	5
5.1	Block ciphers	5
5.2	Stream ciphers.....	6
5.3	Mechanisms using asymmetric techniques	6
A1 5.4	Hash-functions	6
5.5	Message authentication codes (MACs).....	7
5.6	Broadcast authentication protocols	7
5.7	Authenticated encryption	7 A1
Annex A (informative) Selection criteria for inclusion of mechanisms in ISO/IEC 29192		8
Annex B (informative) Obtaining metrics for hardware implementation comparison		9
Annex C (normative) Metrics for hardware targeted block and stream ciphers		12
Annex D (informative) Gate equivalents		13
Bibliography.....		14

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29192-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 29192 consists of the following parts, under the general title *Information technology — Security techniques — Lightweight cryptography*:

- *Part 1: General*
- *Part 2: Block ciphers*
- *Part 3: Stream ciphers*
- *Part 4: Mechanisms using asymmetric techniques*

Further parts may follow.

Introduction

ISO/IEC 29192 is a multi-part International Standard that specifies lightweight cryptography for the purposes of data confidentiality, authentication, identification, non-repudiation, and key exchange. Lightweight cryptography is suitable in particular for constrained environments. The constraints normally encountered can be any of the following:

- chip area;
- energy consumption;
- program code size and RAM size;
- communication bandwidth;
- execution time.

The purpose of ISO/IEC 29192 is to specify standardized mechanisms which are suitable for lightweight cryptographic applications, including radiofrequency identification (RFID) tags, smart cards (e.g. contactless applications), secure batteries, health-care systems (e.g. Body Area Networks), sensor networks, etc.

This part of ISO/IEC 29192 sets the security requirements, classification requirements and implementation requirements of mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.

Lightweight cryptography delivers adequate security in the context for which it is intended. The cryptographic mechanisms standardized in ISO/IEC 29192 provide their full security strength if they are used within the limitations of the mechanisms as specified.

EXAMPLE For a block cipher with a block size of n bits and a key size of k bits, when limiting the use of the block cipher to encrypting no more than $2^{n/2}$ blocks of plaintext under a single key in say counter mode, it will provide k -bit security. The security degrades with more than $2^{n/2}$ blocks.

There are overlaps in some security techniques between ISO/IEC 29192 and existing standards such as ISO/IEC 18033, ISO/IEC 9798, and ISO/IEC 11770. The exclusion of particular mechanisms does not imply that these mechanisms are not suitable for lightweight cryptography. The criteria used to select the cryptographic mechanisms specified in subsequent parts of ISO/IEC 29192 are described in Annex A.

