INTERNATIONAL STANDARD

ISO/IEC 29192-2

First edition
2012-01-15

Information technology — Security techniques — Lightweight cryptography

Part 2: Block ciphers

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

Partie 2: Chiffrements par blocs

Reference number
ISO/IEC 29192-2:2012(E)

COPYRIGHT PROTECTED DOCUMENT

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

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.

ISO/IEC 29192-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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

This part of ISO/IEC 29192 specifies block ciphers suitable for lightweight cryptography, which are tailored for implementation in constrained environments.

ISO/IEC 29192-1 specifies the requirements for lightweight cryptography.

A block cipher maps blocks of *n* bits to blocks of *n* bits, under the control of a key of *k* bits.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holder of these patent rights has assured ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of these patent rights is registered with ISO and IEC. Information may be obtained from:

Sony Corporation
System Technologies Laboratories
Attn Masanobu Katagi
Gotenyama Tec. 5-1-12 Kitashinagwa Shinagawa-ku
Tokyo
141-0001 Japan
Tel. +81-3-5448-3701
Fax +81-3-5448-6438
E-mail Masanobu.Katagi@jp.sony.com

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Lightweight cryptography

Part 2:
Block ciphers

1 Scope

This part of ISO/IEC 29192 specifies two block ciphers suitable for applications requiring lightweight cryptographic implementations:

— PRESENT: a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits;

— CLEFIA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.

2 Normative references

There are no normative references for this part of ISO/IEC 29192.