

First edition  
2016-08-01

---

---

# Information technology — Security techniques — Lightweight cryptography —

## Part 5: Hash-functions

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

*Partie 5: Fonctions de hachage*

---

---

Reference number  
ISO/IEC 29192-5:2016(E)



This is a preview of "ISO/IEC 29192-5:2016". Click [here](#) to purchase the full version from the ANSI store.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of "ISO/IEC 29192-5:2016". Click here to purchase the full version from the ANSI store.

## Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols</b> .....	<b>3</b>
<b>5 Lightweight hash-functions optimized for hardware implementations</b> .....	<b>3</b>
5.1 General.....	3
5.2 PHOTON.....	3
5.2.1 General.....	3
5.2.2 PHOTON specific notation.....	4
5.2.3 Domain extension algorithm.....	4
5.2.4 Internal permutation.....	5
5.3 SPONGENT.....	10
5.3.1 General.....	10
5.3.2 SPONGENT specific notation.....	10
5.3.3 Domain extension algorithm.....	10
5.3.4 Internal permutation.....	11
<b>6 Lightweight hash-functions optimized for software implementations</b> .....	<b>12</b>
6.1 General.....	12
6.2 Lesamnta-LW.....	13
6.2.1 General.....	13
6.2.2 Message padding.....	13
6.2.3 Lesamnta-LW specific notation.....	13
6.2.4 Compression function and domain extension.....	13
6.2.5 Block cipher.....	14
<b>Annex A (normative) Object identifiers</b> .....	<b>17</b>
<b>Annex B (informative) Numerical examples</b> .....	<b>19</b>
<b>Annex C (informative) Feature tables</b> .....	<b>23</b>
<b>Bibliography</b> .....	<b>26</b>

## 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.

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](http://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](http://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology, 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*
- *Part 5: Hash-functions*

Further parts may follow.

This is a preview of "ISO/IEC 29192-5:2016". Click here to purchase the full version from the ANSI store.

## Introduction

This part of ISO/IEC 29192 specifies lightweight hash-functions, which are tailored for implementation in constrained environments.

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

A hash-function maps an arbitrary string of bits to a fixed-length string of bits.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 29192 may involve the use of patents. The ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world.

In this respect, the statements of the holders of these patent rights are registered with the ISO and IEC. Information may be obtained from the following:

Nanyang Technological University - NTUitive Pte Ltd

16 Nanyang Drive, #01-109, Innovation Centre, Singapore 637722

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.

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.