

---

---

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

**Part 1:  
General**

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

*Partie 1: Généralités*



**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	iv
Introduction.....	v
<b>1 Scope .....</b>	<b>1</b>
<b>2 Terms and definitions .....</b>	<b>1</b>
<b>3 Categories of constraints for lightweight cryptography .....</b>	<b>2</b>
<b>3.1 Chip area .....</b>	<b>2</b>
<b>3.2 Energy consumption.....</b>	<b>2</b>
<b>3.3 Program code size and RAM size .....</b>	<b>2</b>
<b>3.4 Communication bandwidth .....</b>	<b>2</b>
<b>3.5 Execution time .....</b>	<b>3</b>
<b>4 Requirements.....</b>	<b>3</b>
<b>4.1 Security requirements.....</b>	<b>3</b>
<b>4.2 Classification requirements .....</b>	<b>3</b>
<b>4.3 Implementation requirements .....</b>	<b>4</b>
<b>5 Lightweight cryptographic mechanisms .....</b>	<b>5</b>
<b>5.1 Block ciphers .....</b>	<b>5</b>
<b>5.2 Stream ciphers.....</b>	<b>6</b>
<b>5.3 Mechanisms using asymmetric techniques .....</b>	<b>6</b>
<b>Annex A (informative) Selection criteria for inclusion of mechanisms in ISO/IEC 29192 .....</b>	<b>7</b>
<b>Annex B (informative) Obtaining metrics for hardware implementation comparison .....</b>	<b>8</b>
<b>Annex C (normative) Metrics for hardware targeted block and stream ciphers .....</b>	<b>11</b>
<b>Annex D (informative) Gate equivalents .....</b>	<b>12</b>
<b>Bibliography.....</b>	<b>13</b>