

ISO/IEC 29192-1:2012-06 (E)

Information technology - Security techniques - Lightweight cryptography - Part 1: General

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
Annex B (informative) Obtaining metrics for hardware implementation comparison		8
Annex C (normative) Metrics for hardware targeted block and stream ciphers		11
Annex D (informative) Gate equivalents		12
Bibliography		13