

ISO/IEC 29192-2:2019-11 (E)

Information security - Lightweight cryptography - Part 2: Block ciphers

| Contents | | Page |
|---|--|-------------|
| Foreword | | iv |
| Introduction | | v |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 1 |
| 4 | Symbols | 2 |
| 5 | Lightweight block cipher with a block size of 64 bits | 2 |
| 5.1 | General | 2 |
| 5.2 | PRESENT | 2 |
| 5.2.1 | PRESENT algorithm | 2 |
| 5.2.2 | PRESENT specific notation | 2 |
| 5.2.3 | PRESENT encryption | 3 |
| 5.2.4 | PRESENT decryption | 4 |
| 5.2.5 | PRESENT transformations | 4 |
| 5.2.6 | PRESENT key schedule | 5 |
| 6 | Lightweight block ciphers with a block size of 128 bits | 7 |
| 6.1 | General | 7 |
| 6.2 | CLEFIA | 7 |
| 6.2.1 | CLEFIA algorithm | 7 |
| 6.2.2 | CLEFIA specific notation | 7 |
| 6.2.3 | CLEFIA encryption | 7 |
| 6.2.4 | CLEFIA decryption | 8 |
| 6.2.5 | CLEFIA building blocks | 9 |
| 6.2.6 | CLEFIA key schedule | 14 |
| 6.3 | LEA | 24 |
| 6.3.1 | LEA algorithm | 24 |
| 6.3.2 | LEA specific notation | 24 |
| 6.3.3 | LEA encryption | 24 |
| 6.3.4 | LEA decryption | 26 |
| 6.3.5 | LEA key schedule | 27 |
| Annex A (normative) Object identifiers | | 30 |
| Annex B (informative) Numerical examples | | 31 |
| Annex C (informative) Feature tables | | 53 |
| Annex D (informative) A limitation of a block cipher under a single key | | 55 |
| Bibliography | | 56 |