ISO/IEC 29192-2:2012-01 (E)

Information technology - Security techniques - 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 PRESENT 2

6 Lightweight block cipher with a block size of 128 bits 7
6.1 CLEFIA 7

Annex A (normative) Object identifiers 24

Annex B (informative) Test vectors 26

Annex C (informative) Feature table 39

Annex D (informative) A limitation of a block cipher under a single key 40

Bibliography 41