ISO/IEC 18033-7:2022-04 (E)

Information security - Encryption algorithms - Part 7: Tweakable block ciphers

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols 2

5 Requirements on the usage of tweakable block ciphers 3

6 Deoxys-TBC 3
6.1 Deoxys-TBC versions 3
6.2 Deoxys-TBC encryption 4
6.3 Deoxys-TBC decryption 5
6.4 Deoxys-TBC tweakey schedule 6

7 Skinny 7
7.1 Skinny versions 7
7.2 Skinny encryption 8
7.3 Skinny decryption 10
7.4 Skinny tweakey schedule 11

Annex A (informative) Numerical examples 14

Annex B (normative)Objectidentifiers 16

Bibliography 18