ISO/IEC 18033-4:2011-12 (E)

Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 3
4.1 Symbols 3
4.2 Functions 5

5 Framework for stream ciphers 6

6 General models for stream ciphers 6
6.1 Keystream generators 6
6.2 Output functions 7

7 Constructing keystream generators from block ciphers 10
7.1 Block cipher modes for a synchronous keystream generator 10
7.2 Block cipher mode for a self-synchronizing keystream generator 12

8 Dedicated keystream generators 13
8.1 MUGI keystream generator 13
8.2 SNOW 2.0 keystream generator 18
8.3 Rabbit keystream generator 23
8.4 Decimv2 keystream generator 27
8.5 KCipher-2 (K2) keystream generator 33

Annex A (normative) Object Identifiers 43

Annex B (informative) Operations over the finite field GF(2n) 45

Annex C (informative) Examples 46

Annex D (informative) Security information 88

Bibliography 91