

ISO/IEC 18033-4 :2005-07 (E)

Contents

Page

| | |
|---|----|
| Foreword..... | iv |
| Introduction..... | v |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions..... | 1 |
| 4 Symbols and abbreviated terms..... | 4 |
| 4.1 Left-truncation of bits..... | 5 |
| 4.2 Shift operation..... | 6 |
| 4.3 Variable $l(k)$ | 6 |
| 5 General models for stream ciphers | 6 |
| 5.1 Keystream generators..... | 6 |
| 5.1.1 Synchronous keystream generators | 6 |
| 5.1.2 Self-synchronizing keystream generators | 6 |
| 5.2 Output functions | 7 |
| 5.2.1 Binary-additive output function | 7 |
| 5.2.2 MULTI-S01 output function..... | 8 |
| 6 Constructing keystream generators from block ciphers..... | 10 |
| 6.1 Modes of a block cipher for a synchronous keystream generator..... | 10 |
| 6.1.1 OFB mode..... | 11 |
| 6.1.2 CTR mode | 11 |
| 6.2 Mode of a block cipher for a self-synchronizing keystream generator | 12 |
| 6.2.1 CFB mode | 12 |
| 7 Dedicated keystream generators | 13 |
| 7.1 MUGI keystream generator | 13 |
| 7.1.1 Initialization function <i>Init</i> | 14 |
| 7.1.2 Next-state function <i>Next</i> | 15 |
| 7.1.3 Keystream function <i>Strm</i> | 15 |
| 7.1.4 Function ρ_1 | 15 |
| 7.1.5 Function λ_1 | 16 |
| 7.1.6 Function F | 16 |
| 7.1.7 Function S_R | 17 |
| 7.1.8 Function M | 18 |
| 7.2 SNOW 2.0 keystream generator | 18 |
| 7.2.1 Initialization function <i>Init</i> | 19 |
| 7.2.2 Next-state function <i>Next</i> | 20 |
| 7.2.3 Keystream function <i>Strm</i> | 21 |
| 7.2.4 Function T | 21 |
| 7.2.5 Multiplications of α in finite field arithmetic..... | 22 |
| 7.2.6 Multiplications of α^{-1} in finite field arithmetic..... | 22 |
| 7.2.7 Function $FSM(x, y, z)$ | 23 |
| Annex A (informative) Examples..... | 24 |
| A.1 Operations over the finite field $GF(2^n)$ | 24 |
| A.2 Example for MUGI..... | 24 |
| A.2.1 Key, initialization vector, and keystream triplets | 24 |
| A.2.2 Sample internal states..... | 24 |
| A.3 Example for SNOW 2.0 | 30 |
| A.3.1 128-bit key..... | 30 |
| A.3.2 256-bit key..... | 34 |

Annex B (informative) Security information 39
B.1 Security levels of stream ciphers..... 39
B.1.1 Security-efficiency trade-off in MULTI-S01 40
B.2 Implementation examples of dedicated keystream generators..... 40
Annex C (normative) Object identifiers..... 41
Bibliography 43