ISO/IEC 29192-8:2022-09 (E)

Information security - Lightweight cryptography - Part 8: Authenticated encryption

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 3

5 Grain-128A 5
5.1 Introduction to Grain-128A 5
5.2 Internal state 6
5.3 Encryption and MAC generation procedure 7
5.4 Decryption and MAC verification procedure 8
5.5 Sub-functions 9
5.5.1 Initialization function Init 9
5.5.2 MAC Initialization function Imac 10
5.5.3 Next-state function Next 11
5.5.4 Pre-output function Prt 11
5.5.5 Keystream function Strm 11
5.5.6 Function Upmac 12
5.5.7 Function Fmac 12

Annex A (normative)Objectidentifiers 13

Annex B (informative) Numerical examples 14

Annex C (informative) Security considerations 16

Bibliography 17