ISO/IEC 29192-4:2013-06 (E)

Information technology - Security techniques - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 4

5 Unilateral authentication mechanism based on discrete logarithms on elliptic curves 6
5.1 General 6
5.2 Security requirements for the environment 6
5.3 Key production 7
5.4 Unilateral authentication mechanism 8

6 Unilateral authenticated key exchange mechanism based on encryption 9
6.1 General 9
6.2 Security requirements for the environment 10
6.3 Key production 10
6.4 Unilateral authentication exchange 11
6.5 Session-key derivation 12

7 Identity-based signature mechanism 12
7.1 General 12
7.2 Security requirements for the environment 12
7.3 Key production 13
7.4 Sign 13
7.5 Verify 13

Annex A (normative) Object identifiers 14

Annex B (normative) Memory-Computation Trade-Off Technique 15

Annex C (informative) Numerical examples 16

C.1 cryptoGPS mechanism 16
C.1.1 Key production 16
C.1.2 Authentication exchange 16
C.2 ALIKE mechanism 18
C.2.1 Key production 18
C.2.2 Authentication exchange 18
C.2.3 Session-key derivation 19
C.3 Identity-based signature mechanism 19
C.3.1 Key production 19
C.3.2 Sign 20
C.3.3 Verify 21

Annex D (informative) Features 22

Bibliography 25