ISO/IEC 19592-2:2017-10 (E)

Information technology - Security techniques - Secret sharing - Part 2: Fundamental mechanisms

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 2

5 Secret sharing schemes 3
5.1 General 3
5.2 Shamir secret sharing scheme 4
5.2.1 General 4
5.2.2 Parameters 4
5.2.3 Message sharing algorithm 4
5.2.4 Message reconstruction algorithm 4
5.2.5 Properties 4
5.3 Ramp Shamir secret sharing scheme 5
5.3.1 General 5
5.3.2 Parameters 5
5.3.3 Message sharing algorithm 5
5.3.4 Message reconstruction algorithm 6
5.3.5 Properties 6
5.4 Additive secret sharing scheme for a general adversary structure 6
5.4.1 General 6
5.4.2 Parameters 6
5.4.3 Message sharing algorithm 7
5.4.4 Message reconstruction algorithm 7
5.4.5 Properties 7
5.5 Replicated additive secret sharing scheme 7
5.5.1 General 7
5.5.2 Parameters 8
5.5.3 Message sharing algorithm 8
5.5.4 Message reconstruction algorithm 8
5.5.5 Properties 8
5.6 Computational additive secret sharing scheme 8
5.6.1 General 8
5.6.2 Parameters 9
5.6.3 Message sharing algorithm 9
5.6.4 Message reconstruction algorithm 9
5.6.5 Properties 10
5.6.6 Conversion protocol 10

Annex A (informative)Objectidentifiers 12

Annex B (informative) Numerical examples 14

Bibliography 22