Contents

1 Introduction 1
Yuliang Zheng
1.1 Historical Development of Signcryption 1
1.1.1 Coded Modulation 1
1.1.2 Musings on Blending 2
1.1.3 Signcryption 5
1.1.4 Provably Secure Signcryption 7
1.2 Extensions, Standardization, and Future Research Directions 8
1.3 Notation and Security Notions 9
1.3.1 Algorithms and Assignment 10
1.3.2 Signature Schemes 11
1.3.3 Public Key Encryption 14
1.3.4 Symmetric Encryption 16
1.3.5 Message Authentication Codes 18

Part I Security Models for Signcryption

2 Security for Signcryption: The Two-User Model 21
Jee Hea An and Tal Rabin
2.1 Introduction 21
2.2 Definition of Signcryption in the Two-User Setting 23
2.2.1 Two Security Notions in the Two-User Setting 23
2.2.2 Discussions on the Security Notions 28
2.3 Generic Compositions of Signature and Encryption 30
2.3.1 Construction 30
2.3.2 Security of the Parallel Composition Method 31
2.3.3 Security of the Sequential Composition Methods 32
2.4 Multi-user Setting 39
2.4.1 Syntax 39
2.4.2 Security 40
2.4.3 Extending Signcryption 40

Bibliografische Informationen
http://d-nb.info/1004070799

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3 Security for Signcryption: The Multi-User Model 43
Joonsang Baek and Ron Steinfeld
3.1 Introduction 43
3.2 The BSZ Model 44
3.2.1 Confidentiality of Signcryption in the Multi-User BSZ Model 44
3.2.2 Unforgeability of Signcryption in the Multi-User BSZ Model 47
3.2.3 Further Discussions on the Multi-User BSZ Model 50
3.3 Example: The Security of Zheng's Signcryption Scheme in the BSZ Model 51

Part II Signcryption Schemes

4 Signcryption Schemes Based on the Diffie–Hellman Problem 57
Paulo S.L.M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater
4.1 Introduction 57
4.2 Diffie–Hellman Problems 58
4.3 Zheng's Construction and Its Variants 59
4.3.1 Zheng's Original Scheme 59
4.3.2 The Bao–Deng Modification 62
4.3.3 A Modification with Public Verifiability 62
4.4 An Encrypt-then-Sign Composition 63
4.5 A Scheme with Unforgeability Based on Factoring 64
4.6 Schemes with Non-repudiation 66
4.6.1 A DSA-Based Construction 66
4.6.2 A Scheme Built on Schnorr's Signature Scheme 67
4.7 The CM Scheme 68

5 Signcryption Schemes Based on Bilinear Maps 71
Paulo S.L.M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater
5.1 Introduction 71
5.2 Bilinear Map Groups 72
5.3 Assumptions 73
5.4 Signcryption for Anonymous Communications 74
5.4.1 Message Privacy 75
5.4.2 Ciphertext Unforgeability and Signature Unforgeability .. 76
5.4.3 Anonymity 77
5.5 A Tightly Secure Scheme 78
5.5.1 The Scheme 78

5.5.2 Efficiency 79
5.5.3 Security 80
5.6 A Scheme with Short Detachable Signatures 86
5.6.1 Efficiency 88
5.6.2 Anonymous Communications 88
5.6.3 Security 89

6 Signcryption Schemes Based on the RSA Problem 99
Alexander W. Dent and John Malone-Lee
6.1 Introduction 99
6.2 The RSA Transform 100
6.3 Dedicated RSA-Based Signcryption Schemes 101
6.4 Signcryption from Padding Schemes 102
6.4.1 Trapdoor Permutations 102
6.4.2 Extractable Commitments 102
6.4.3 Padding-Based Signcryption Schemes 104
6.4.4 Proof Intuition 109
6.5 Signcryption Based on RSA-TBOS 110
6.5.1 The TBOS Construction 110
6.5.2 Security Proof for the TBOS Signcryption Scheme 112

Part III Construction Techniques

7 Hybrid Signcryption 121
Tor E. Bjørstad
7.1 Background 121
7.1.1 A Brief Word on Notation 123
7.2 Preliminaries 123
7.2.1 The Hybrid Framework 123
7.2.2 Security Criteria for Data Encapsulation Mechanisms 125
7.3 Hybrid Signcryption with Outsider Security 126
7.3.1 An Outsider-Secure Signcryption KEM 126
7.3.2 Security Criteria for Outsider-Secure Signcryption KEMs 127
7.3.3 Security of the SKEM + DEM Construction 130
7.3.4 Outsider-Secure Hybrid Signcryption in Practice 133
7.4 Hybrid Signcryption with Insider Security 136
7.4.1 From Outsider to Insider Security 136
7.4.2 Signcryption Tag-KEMs 138
7.4.3 Security Criteria for Signcryption Tag-KEMs 140
7.4.4 Security of the SCTK+DEM Construction 143
7.4.5 Insider-Secure Hybrid Signcryption in Practice 146

8 Concealment and Its Applications to Authenticated Encryption 149
Yevgeniy Dodis
8.1 Introduction 149
8.1.1 Domain Extension of Authenticated Encryption 150
8.1.2 Remotely Keyed Authenticated Encryption 152
8.2 Definition of Concealment 155
8.2.1 Syntax 155
8.2.2 Security of Concealment 156
8.2.3 Relaxed Concealments 157
8.2.4 Super-Relaxed Concealments 157
8.2.5 Comparison to Commitment 157
8.3 Constructing Concealment Schemes 158
8.3.1 Achieving Hiding 158
8.3.2 Achieving Binding 159
8.3.3 Necessity of Assumptions 162
8.4 Applications to Authenticated Encryption 163
8.4.1 Definition of Authenticated Encryption 164
8.4.2 Authenticated Encryption of Long Messages 166
8.4.3 Remotely Keyed Authenticated Encryption 169

9 Parallel Signcryption 175
Josef Pieprzyk and David Pointcheval
9.1 Introduction 175
9.2 Concept of Parallel Signcryption 175
9.3 Overview of Constructions 176
9.4 Generic Parallel Signcryption 178
9.4.1 Description of the Scheme 178
9.4.2 Security Analysis 180
9.5 Optimal Parallel Signcryption 185
9.5.1 Description of the Scheme 185
9.5.2 Security Analysis 187

Part IV Extensions of Signcryption

10 Identity-Based Signcryption 195
Xavier Boyen
10.1 Introduction 195
10.1.1 Identity-Based Cryptography 195
10.1.2 Advantages and Disadvantages 197
10.1.3 From IBE to Signcryption 199
10.1.4 Specifying an IBSC System 200
10.1.5 Concrete IBSC from Pairings 201
10.2 The Identity-Based Signcryption Primitive 202

10.3 Security Definitions 203
10.3.1 Message Confidentiality 206
10.3.2 Signature Non-repudiation 207
10.3.3 Ciphertext Unlinkability 208
10.3.4 Ciphertext Authentication 209
10.3.5 Ciphertext Anonymity 210
10.4 A Concrete IBSC Scheme 211
10.4.1 The Boneh–Franklin Framework 211
10.4.2 Fully Secure IBSC Construction 212
10.4.3 A Performance/Security Trade-Off 215
10.4.4 Signcrypting for Multiple Recipients 215

11 Key Establishment Using Signcryption Techniques 217
Alexander W. Dent
11.1 Introduction 217
11.2 Formal Security Models for Key Establishment 219
11.2.1 Motivation 219
11.2.2 Sessions 220
11.2.3 The Formal Security Model 221
11.2.4 Entity Authentication 223
11.2.5 Forward Secrecy 224
11.2.6 Key Compromise Impersonation Attacks 224
11.2.7 Notation 224
11.3 Key Transport 225
11.4 Key Establishment Based on Zheng's Signcryption Scheme 226
11.5 Key Agreement Based on Signcryption KEMs 227
11.5.1 Key Agreement Based on Signcryption KEMs 229
11.5.2 Key Agreement Based on Signcryption Tag-KEMs 230
11.5.3 Security Proof for the Bjørstad–Dent Protocol 232
11.6 Key Establishment Based on Timestamps 239

12 Applications of Signcryption 241
Yang Cui and Goichiro Hanaoka
12.1 Application Fields of Signcryption 241
12.2 Example Applications of Signcryption 242
12.2.1 Secure Multicasting Over the Internet 243
12.2.2 Authenticated Key Recovery 246
12.2.3 Secure ATM Networks 248
12.2.4 Secure Routing for Mobile Ad Hoc Networks 249
12.2.5 Encrypted and Authenticated E-mail by Firewalls 251
12.2.6 Signcryption in Secure VoIP 252
12.2.7 Applications to Electronic Payment 253

References 257

Index 269