Contents

Foreword **xi**

Preface **xiii**

Summary **xvii**

List of Figures **xxiii**

1 Introduction **1**

1.1 Digital certificates and PKIs 1

1.1.1 From paper-based to digital certificates 1

1.1.2 Identity certificates 3

1.1.3 Central database paradigm 6

1.1.4 Attribute certificates 9

1.1.5 Certificate revocation and validation 13

1.1.6 Smartcard integration 15

1.2 Privacy issues 20

1.2.1 Privacy dangers 20

1.2.2 Previous privacy-protection efforts and their shortcomings . 25

1.2.3 Desirable privacy properties 30

1.3 Outlook 32

1.3.1 Basic building blocks 32

1.3.2 Additional privacy techniques 34

1.3.3 Security techniques 35

1.3.4 Smartcard integration 37

1.3.5 Security and privacy guarantees 39

1.3.6 Applicability 40

2 Cryptographic Preliminaries **41**

2.1 Notation, terminology, and conventions 41

2.1.1 Basic notation 41

2.1.2 Algorithms, security parameters, and probability 42
2.1.3 Interactive algorithms and protocols 44
2.1.4 Attack models 45
2.1.5 Security reductions and the random oracle model 48
2.2 One-way functions 49
2.2.1 Definition 49
2.2.2 The DL function 51
2.2.3 The RSA function 56
2.3 Collision-intractable functions 58
2.3.1 Definition 58
2.3.2 The DLREP function 59
2.3.3 The RSAREP function 62
2.3.4 Comparison 65
2.4 Proofs of knowledge 66
2.4.1 Definition 66
2.4.2 Security for the prover 67
2.4.3 Proving knowledge of a DL-representation 71
2.4.4 Proving knowledge of an RSA-representation 75
2.5 Digital signatures 77
2.5.1 Definition 77
2.5.2 From proofs of knowledge to digital signature schemes . . . 79
2.5.3 Digital signatures based on the DLREP function 81
2.5.4 Digital signatures based on the RSAREP function 84
2.6 Digital certificates 86
2.6.1 Definition of public-key certificates 86
2.6.2 Definition of secret-key certificates 87
2.6.3 Comparison 89
2.7 Bibliographic notes 90

3 Showing Protocols with Selective Disclosure 91
3.1 Introduction 91
3.2 How to commit 92
3.3 Formulae with zero or more “AND” connectives 93
3.3.1 Technique based on the DLREP function 93
3.3.2 Technique based on the RSAREP function 105
3.4 Formulae with one “NOT” connective 108
3.4.1 Technique based on the DLREP function 108
3.4.2 Technique based on the RSAREP function 118
3.5 Atomic formulae connected by “OR” connectives 119
3.5.1 Technique based on the DLREP function 119
3.5.2 Technique based on the RSAREP function 123
3.6 Demonstrating arbitrary Boolean formulae 123

3.6.1 Technique based on the DLREP function 123
3.6.2 Technique based on the RSAREP function 126
3.7 Optimizations and extensions 128
3.8 Bibliographic notes 130

4 Restrictive Blind Issuing Protocols 131
4.1 Restrictive blinding 131
4.2 Practical constructions 134
4.2.1 Restrictive blinding based on the DLREP function 135
4.2.2 Restrictive blinding based on the RSAREP function 139
4.2.3 Comparison 140
4.3 Analysis 146
4.3.1 Completeness 146
4.3.2 Privacy for the receiver 147
4.3.3 Security for the Certificate Authority 149
4.3.4 Additional properties 160
4.4 Parallelization of protocol executions 162
4.4.1 Masking the initial witness 163
4.4.2 Swapping exponents in the verification relation 166
4.5 Other certificate schemes 171
4.5.1 DSA-like certificates 171
4.5.2 Certificates based on Chaum-Pedersen signatures 175
4.6 Bibliographic notes 178

5 Combining Issuing and Showing Protocols 181
5.1 Integration 181
5.1.1 Making the match 181
5.1.2 Coping with delegation 185
5.2 Privacy improvements for certificate holders 189
5.2.1 Issuing protocol techniques 189
5.2.2 Showing protocol techniques 191
5.3 Privacy improvements for certificate verifiers 193
5.4 Limited-show certificates 197
5.4.1 Static one-show certificates 197
5.4.2 Dynamic one-show certificates 201
5.4.3 Increasing the threshold 207
5.5 Security improvements 208
5.5.1 Benefits of encoding identifiers 208
5.5.2 How to discourage lending 211
5.5.3 Non-repudiation 212
5.5.4 How to discourage discarding 213
5.5.5 Guarding the secret key of the Certificate Authority 213

5.6 Bibliographic notes 216

6 Smartcard Integration 219
6.1 Shortcomings of the smartcard-only paradigm 219
6.1.1 Privacy dangers 219
6.1.2 Other shortcomings 223
6.2 Combining smartcards and software-only devices 224
6.2.1 Benefits 225
6.2.2 How not to cope with subliminal channels 227
6.3 Secure smartcard integration 230
6.3.1 Technique based on the DLREP function 230
6.3.2 Technique based on the RSAREP function 236
6.4 Privacy protection 238
6.4.1 Inflow prevention 239
6.4.2 Outflow prevention 240
6.4.3 Prevention of other data leakage channels 242
6.4.4 Restricting the level of privacy protection 245
6.5 Other techniques 247
6.5.1 Implementation in low-cost smartcards 248
6.5.2 Returning certificates 250
6.5.3 How to discourage remote lending 251
6.5.4 Bearer certificates 252
6.5.5 Loose ends 253
6.6 Bibliographic notes 254

Epilogue: The Broader Perspective 257

References 273

Curriculum Vitae 307

Index 307