Contents

Introduction to post-quantum cryptography

Daniel J. Bernstein 1
1 Is cryptography dead? 1
2 A taste of post-quantum cryptography 6
3 Challenges in post-quantum cryptography 11
4 Comparison to quantum cryptography 13

Quantum computing

Sean Hallgren, Ulrich Vollmer 15
1 Classical cryptography and quantum computing 15
2 The computational model 19
3 The quantum Fourier transform 22
4 The hidden subgroup problem 25
5 Search algorithms 29
6 Outlook 31
References 32

Hash-based Digital Signature Schemes

Johannes Buchmann, Erik Dahmen, Michael Szydlo 35
1 Hash based one-time signature schemes 36
2 Merkle's tree authentication scheme 40
3 One-time key-pair generation using an PRNG 44
4 Authentication path computation 46
5 Tree chaining 69
6 Distributed signature generation 73
7 Security of the Merkle Signature Scheme 81
References 91

Code-based cryptography

Raphael Overbeck, Nicolas Sendrier 95
1 Introduction 95
2 Cryptosystems 96

3 The security of computing syndromes as one-way function 106
4 Codes and structures 116
5 Practical aspects 127
6 Annex 137
References 141

Lattice-based Cryptography

Daniele Micciancio, Oded Regev 147
1 Introduction 147
2 Preliminaries 152
3 Finding Short Vectors in Random q-ary Lattices 154
4 Hash Functions 157
5 Public Key Encryption Schemes 165
6 Digital Signature Schemes 180
7 Other Cryptographic Primitives 185
8 Open Questions 186
References 187

Multivariate Public Key Cryptography

Jintai Ding, Bo-Yin Yang 193
1 Introduction 193
2 The Basics of Multivariate PKCs 194
3 Examples of Multivariate PKCs 198
4 Basic Constructions and Variations 202
5 Standard Attacks 215
6 The Future 229
References 234

Index 243