QUANTUM CRYPTOGRAPHY AND SECRET-KEY DISTILLATION

GILLES VAN ASSCHE

CAMBRIDGE
UNIVERSITY PRESS

Contents

Foreword *page* ix
N. J. Cerf and S. W. McLaughlin
Preface xi
Acknowledgments xiii

1 Introduction 1
1.1 A first tour of quantum key distribution 4
1.2 Notation and conventions 12

2 Classical cryptography 15
2.1 Confidentiality and secret-key ciphers 15
2.2 Secret-key authentication 26
2.3 Public-key cryptography 29
2.4 Conclusion 33

3 Information theory 35
3.1 Source coding 35
3.2 Joint and conditional entropies 40
3.3 Channel coding 41
3.4 Rényi entropies 43
3.5 Continuous variables 45
3.6 Perfect secrecy revisited 46
3.7 Conclusion 48

4 Quantum information theory 49
4.1 Fundamental definitions in quantum mechanics 49
4.2 Qubits and qubit pairs 52
4.3 Density matrices and quantum systems 54
4.4 Entropies and coding 55
4.5 Particularity of quantum information 56
4.6 Quantum optics 58

4.7 Conclusion 60

5 Cryptosystems based on quantum key distribution 63
5.1 A key distribution scheme 63
5.2 A secret-key encryption scheme 70
5.3 Combining quantum and classical cryptography 73
5.4 Implementation of a QKD-based cryptosystem 77
5.5 Conclusion 84

6 General results on secret-key distillation 85
6.1 A two-step approach 85
6.2 Characteristics of distillation techniques 87
6.3 Authenticated one-shot secret-key distillation 88
6.4 Authenticated repetitive secret-key distillation 92
6.5 Unauthenticated secret-key distillation 96
6.6 Secret-key distillation with continuous variables 98
6.7 Conclusion 100

7 Privacy amplification using hash functions 101
7.1 Requirements 101
7.2 Universal families suitable for privacy amplification 104
7.3 Implementation aspects of hash functions 107
7.4 Conclusion 112

8 Reconciliation 113
8.1 Problem description 113
8.2 Source coding with side information 116
8.3 Binary interactive error correction protocols 124
8.4 Turbo codes 129
8.5 Low-density parity-check codes 137
8.6 Conclusion 140

9 Non-binary reconciliation 141
9.1 Sliced error correction 141
9.2 Multistage soft decoding 148
9.3 Reconciliation of Gaussian key elements 149
9.4 Conclusion 158

10 The BB84 protocol 159
10.1 Description 159
10.2 Implementation of BB84 160
10.3 Eavesdropping and secret key rate 170
10.4 Conclusion 181

11 Protocols with continuous variables 183
11.1 From discrete to continuous variables 183
11.2 A protocol with squeezed states 184
11.3 A protocol with coherent states: the GG02 protocol 189
11.4 Implementation of GG02 194
11.5 GG02 and secret-key distillation 198
11.6 Conclusion 203

12 Security analysis of quantum key distribution 205
12.1 Eavesdropping strategies and secret-key distillation 205
12.2 Distillation derived from entanglement purification 207
12.3 Application to the GG02 protocol 221
12.4 Conclusion 244

Appendix: symbols and abbreviations 245
Bibliography 249
Index 259