

Contents

1	Introduction	1
	C. Kollmitzer	
2	Preliminaries	3
	M. Pivk	
2.1	Quantum Information Theory	3
2.2	Unconditional Secure Authentication	14
2.3	Entropy	19
	References	21
3	Quantum Key Distribution	23
	M. Pivk	
3.1	Quantum Channel	24
3.2	Public Channel	27
3.3	QKD Gain	45
3.4	Finite Resources	46
	References	46
4	Adaptive Cascade	49
	S. Rass and C. Kollmitzer	
4.1	Introduction	49
4.2	Error Correction and the Cascade Protocol	49
4.3	Adaptive Initial Block-Size Selection	52
4.4	Fixed Initial Block-Size	53
4.5	Dynamic Initial Block-Size	56
4.6	Examples	65
4.7	Summary	66
	References	68
5	Attack Strategies on QKD Protocols	71
	S. Schauer	
5.1	Introduction	72

5.2 Attack Strategies in an Ideal Environment 73

5.3 Individual Attacks in an Realistic Environment 89

References 94

6 QKD Systems 97

 M. Suda

 6.1 Introduction 97

 6.2 QKD Systems 98

 6.3 Summary 117

 References 119

7 Statistical Analysis of QKD Networks in Real-Life Environment 123

 K. Lessiak and J. Pilz

 7.1 Statistical Methods 123

 7.2 Results of the Experiments 127

 7.3 Statistical Analysis 142

 7.4 Summary 147

 References 148

8 QKD Networks Based on Q3P 151

 O. Maurhart

 8.1 QKD Networks 151

 8.2 PPP 154

 8.3 Q3P 155

 8.4 Routing 167

 8.5 Transport 168

 References 170

9 Quantum-Cryptographic Networks from a Prototype to the Citizen 173

 P. Schartner and C. Kollmitzer

 9.1 The SECOQC Project 173

 9.2 How to Bring QKD into the “Real” Life 176

 9.3 Resumee 182

 References 183

10 The Ring of Trust Model 185

 C. Kollmitzer and C. Moesslacher

 10.1 Introduction 185

 10.2 Model of the Point of Trust Architecture 186

 10.3 Communication in the Point of Trust Model 186

 10.4 Exemplified Communications 194

 10.5 A Medical Information System Based on the Ring of Trust 204

 References 210

Index 211