

Contents

<i>Preface</i>	<i>page xi</i>
<i>Notation</i>	<i>xiii</i>
<i>List of abbreviations</i>	<i>xv</i>
Part I Preliminaries	1
1 An information-theoretic approach to physical-layer security	3
1.1 Shannon’s perfect secrecy	4
1.2 Secure communication over noisy channels	6
1.3 Channel coding for secrecy	7
1.4 Secret-key agreement from noisy observations	8
1.5 Active attacks	9
1.6 Physical-layer security and classical cryptography	10
1.7 Outline of the rest of the book	11
2 Fundamentals of information theory	13
2.1 Mathematical tools of information theory	13
2.1.1 Useful bounds	13
2.1.2 Entropy and mutual information	14
2.1.3 Strongly typical sequences	18
2.1.4 Weakly typical sequences	21
2.1.5 Markov chains and functional dependence graphs	22
2.2 The point-to-point communication problem	23
2.2.1 Point-to-point communication model	24
2.2.2 The source coding theorem	26
2.2.3 The channel coding theorem	29
2.3 Network information theory	32
2.3.1 Distributed source coding	33
2.3.2 The multiple-access channel	37
2.3.3 The broadcast channel	40
2.4 Bibliographical notes	44

Part II Information-theoretic security	47
3 Secretory capacity	49
3.1 Shannon’s cipher system	49
3.2 Secure communication over a noisy channel	53
3.3 Perfect, weak, and strong secrecy	55
3.4 Wyner’s wiretap channel	58
3.4.1 Achievability proof for the degraded wiretap channel	65
3.4.2 Converse proof for the degraded wiretap channel	76
3.5 Broadcast channel with confidential messages	78
3.5.1 Channel comparison	83
3.5.2 Achievability proof for the broadcast channel with confidential messages	90
3.5.3 Converse proof for the broadcast channel with confidential messages	98
3.6 Multiplexing and feedback	103
3.6.1 Multiplexing secure and non-secure messages	103
3.6.2 Feedback and secrecy	104
3.7 Conclusions and lessons learned	108
3.8 Bibliographical notes	110
4 Secret-key capacity	112
4.1 Source and channel models for secret-key agreement	113
4.2 Secret-key capacity of the source model	118
4.2.1 Secret-key distillation based on wiretap codes	120
4.2.2 Secret-key distillation based on Slepian–Wolf codes	121
4.2.3 Upper bound for secret-key capacity	127
4.2.4 Alternative upper bounds for secret-key capacity	129
4.3 Sequential key distillation for the source model	134
4.3.1 Advantage distillation	136
4.3.2 Information reconciliation	143
4.3.3 Privacy amplification	148
4.4 Secret-key capacity of the channel model	162
4.5 Strong secrecy from weak secrecy	166
4.6 Conclusions and lessons learned	169
4.7 Appendix	170
4.8 Bibliographical notes	174
5 Security limits of Gaussian and wireless channels	177
5.1 Gaussian channels and sources	177
5.1.1 Gaussian broadcast channel with confidential messages	177
5.1.2 Multiple-input multiple-output Gaussian wiretap channel	185
5.1.3 Gaussian source model	190

	Contents	ix
5.2	Wireless channels	193
5.2.1	Ergodic-fading channels	195
5.2.2	Block-fading channels	203
5.2.3	Quasi-static fading channels	206
5.3	Conclusions and lessons learned	210
5.4	Bibliographical notes	210
Part III	Coding and system aspects	213
6	Coding for secrecy	215
6.1	Secrecy and capacity-achieving codes	216
6.2	Low-density parity-check codes	217
6.2.1	Binary linear block codes and LDPC codes	217
6.2.2	Message-passing decoding algorithm	220
6.2.3	Properties of LDPC codes under message-passing decoding	222
6.3	Secrecy codes for the binary erasure wiretap channel	223
6.3.1	Algebraic secrecy criterion	225
6.3.2	Coset coding with dual of LDPC codes	228
6.3.3	Degrading erasure channels	229
6.4	Reconciliation of binary memoryless sources	231
6.5	Reconciliation of general memoryless sources	234
6.5.1	Multilevel reconciliation	235
6.5.2	Multilevel reconciliation of Gaussian sources	239
6.6	Secure communication over wiretap channels	242
6.7	Bibliographical notes	245
7	System aspects	247
7.1	Basic security primitives	248
7.1.1	Symmetric encryption	248
7.1.2	Public-key cryptography	249
7.1.3	Hash functions	250
7.1.4	Authentication, integrity, and confidentiality	251
7.1.5	Key-reuse and authentication	251
7.2	Security schemes in the layered architecture	253
7.3	Practical case studies	256
7.4	Integrating physical-layer security into wireless systems	260
7.5	Bibliographical notes	265
Part IV	Other applications of information-theoretic security	267
8	Secrecy and jamming in multi-user channels	269
8.1	Two-way Gaussian wiretap channel	270
8.2	Cooperative jamming	275
8.3	Coded cooperative jamming	283

x	Contents	
	8.4 Key-exchange	289
	8.5 Bibliographical notes	291
9	Network-coding security	293
	9.1 Fundamentals of network coding	293
	9.2 Network-coding basics	295
	9.3 System aspects of network coding	297
	9.4 Practical network-coding protocols	299
	9.5 Security vulnerabilities	302
	9.6 Securing network coding against passive attacks	303
	9.7 Countering Byzantine attacks	306
	9.8 Bibliographical notes	309
	<i>References</i>	311
	<i>Author index</i>	323
	<i>Subject index</i>	326