

# Contents

	<i>List of Contributors</i>	page xv
	<i>Preface</i>	xix
<b>Part I</b>	<b>Theoretical Foundations</b>	1
<b>1</b>	<b>Effective Secrecy: Reliability, Confusion, and Stealth</b>	3
	J. Hou, G. Kramer, and M. Bloch	
1.1	Introduction	3
1.2	Preliminaries	5
1.2.1	Terminology	5
1.2.2	Notation	6
1.2.3	Wiretap Channel	6
1.3	Effective Secrecy Capacity	7
1.3.1	Examples	8
1.3.2	Achievability	9
1.3.3	Converse	13
1.3.4	Choice of Security Measures	15
1.4	Hypothesis Testing	16
1.5	Conclusion	18
	<i>References</i>	19
<b>2</b>	<b>Error-Free Perfect Secrecy Systems</b>	21
	S.-W. Ho, T. Chan, A. Grant, and C. Uduwerelle	
2.1	Introduction	21
2.1.1	Organization	24
2.1.2	Notation	25
2.2	Error-Free Perfect Secrecy Systems	25
2.3	Residual Secret Randomness and Expected Key Consumption	30
2.3.1	The First Justification of $H(R U, X)$	32
2.3.2	The Second Justification of $H(R U, X)$	36
2.3.3	Some Properties of $I(R; U, X)$ and $I(R; X)$	37

2.4	Tradeoff between Key Consumption and Number of Channel Uses	38
2.4.1	Minimal Expected Key Consumption	39
2.4.2	Minimal Number of Channel Uses	45
2.4.3	The Fundamental Tradeoff	46
2.5	Proof of Theorem 2.8	47
2.6	Conclusion	48
	<i>References</i>	50
<b>3</b>	<b>Secure Source Coding</b>	<b>51</b>
	P. Cuff and C. Schieler	
3.1	Introduction	51
3.2	Lossless Compression, Perfect Secrecy	53
3.2.1	Discrete Memoryless Source	55
3.3	Lossless Compression, Imperfect Secrecy	58
3.3.1	Rate–Distortion Theory	58
3.3.2	Henchman	62
3.3.3	Repeated Guessing	64
3.3.4	Best Guess	65
3.4	Lossy Compression, Imperfect Secrecy	67
3.4.1	Rate–Distortion Theory	68
3.4.2	Henchman	70
3.5	Equivocation	72
	<i>References</i>	75
<b>4</b>	<b>Networked Secure Source Coding</b>	<b>77</b>
	K. Kittichokechai, T. J. Oechtering, and M. Skoglund	
4.1	Introduction	77
4.1.1	Information Theoretic Measure for Privacy	78
4.1.2	Fundamental Tradeoff	78
4.1.3	Models	79
4.2	Lossy Source Coding in the Presence of an Eavesdropper	81
4.2.1	Problem Setup	81
4.2.2	Rate–Distortion–Leakage Tradeoff Result	82
4.2.3	Example	84
4.3	Network with One Helper	85
4.3.1	Eavesdropper Observes Helper Description Link	85
4.3.2	Eavesdropper Observes Source Description Link	90
4.4	Network with an Intermediate Node	92
4.4.1	Models	93
4.4.2	Problem Setup	93
4.4.3	Rate–Distortion–Leakage Tradeoff Results	94
4.5	Network with Reconstruction Privacy	96
4.5.1	End-User Privacy at Eavesdropper	98

4.5.2	Causal Side Information	100
4.5.3	Example	101
4.6	Open Problems and Concluding Remark	102
	<i>References</i>	104
<b>Part II</b>	<b>Secure Communication</b>	107
<b>5</b>	<b>Secrecy Rate Maximization in Gaussian MIMO Wiretap Channels</b>	109
	S. Loyka and C. D. Charalambous	
5.1	Introduction	109
5.2	MIMO Wiretap Channel	111
5.3	Rank-1 Solution	113
5.4	Full-Rank Solution	113
5.5	Weak Eavesdropper	117
5.6	Isotropic Eavesdropper and Capacity Bounds	120
5.6.1	High SNR Regime	124
5.6.2	When Is the Eavesdropper Negligible?	125
5.6.3	Low SNR Regime	126
5.7	Omnidirectional Eavesdropper	126
5.8	Identical Right Singular Vectors	127
5.9	When Is ZF Signaling Optimal?	129
5.10	When Is Standard Water-Filling Optimal?	130
5.11	When Is Isotropic Signaling Optimal?	131
5.12	An Algorithm for Global Maximization of Secrecy Rates	131
5.13	Appendix	135
5.13.1	Proof of Theorem 5.4	135
5.13.2	Proof of Theorem 5.5	136
	<i>References</i>	137
<b>6</b>	<b>MIMO Wiretap Channels</b>	140
	M. Nafea and A. Yener	
6.1	Introduction	140
6.2	Secrecy Capacity of the MIMO Wiretap Channel	142
6.3	High-SNR Secrecy Capacity for the MIMO Wiretap Channel	146
6.4	MIMO Wiretap Channel with a Cooperative Jammer	148
6.4.1	Converse for Theorem 6.3	150
6.4.2	Achievability for Theorem 6.3	153
6.4.3	Interpretation of Results	158
6.5	MIMO Wiretap Channel with Unknown Eavesdropper Channel	159
6.5.1	Proof of Theorem 6.4	161
6.6	MIMO MAC Gaussian Wiretap Channel with Unknown Eavesdropper Channel	175
6.7	Conclusions	178
	<i>References</i>	178

<b>7</b>	<b>MISO Wiretap Channel with Strictly Causal CSI: A Topological Viewpoint</b>	181
	Z. H. Awan and A. Sezgin	
7.1	Introduction	181
7.2	State of the Art and Preliminaries	181
7.3	Secrecy Capacity Characterization	182
7.4	Secure Degrees of Freedom	184
	7.4.1 Impact of CSIT	184
	7.4.2 Topological Diversity	189
7.5	GSDoF of MISO Wiretap Channel with Delayed CSIT	189
	7.5.1 Upper Bound	191
	7.5.2 Fixed Topology ( $\lambda_{11} = 1$ )	192
	7.5.3 Fixed Topology ( $\lambda_{1\alpha} = 1$ )	192
7.6	Discussion and Directions for Future Work	194
	7.6.1 MISO Broadcast Channel with Topology	194
	7.6.2 Synergistic Benefits of CSIT with Topology	194
	7.6.3 Extension to $K$ -User Case	195
7.7	Appendix	195
	7.7.1 Entropy	195
	7.7.2 Degrees of Freedom	196
	7.7.3 Generalized Degrees of Freedom	196
	<i>References</i>	197
<b>8</b>	<b>Physical-Layer Security with Delayed, Hybrid, and Alternating Channel State Knowledge</b>	200
	P. Mukherjee, R. Tandon, and S. Ulukus	
8.1	Introduction	200
8.2	The MISO Broadcast Channel	202
	8.2.1 Modeling the Quality of CSIT	203
	8.2.2 Security Requirements	204
	8.2.3 A Degrees-of-Freedom Perspective	204
8.3	The MISO BCCM in Homogeneous CSIT States	205
	8.3.1 Perfect CSIT from Both Users (PP)	205
	8.3.2 No CSIT from Any User (NN)	206
	8.3.3 Delayed CSIT from Both Users (DD)	206
8.4	The MISO BCCM in Hybrid CSIT States	211
	8.4.1 Achievable Schemes for States PN and DN	211
	8.4.2 Converse Tools	213
8.5	The MISO BCCM in Alternating CSIT States	214
	8.5.1 Achievability	220
8.6	Conclusions and Open Problems	225
	<i>References</i>	226

<b>9</b>	<b>Stochastic Orders, Alignments, and Ergodic Secrecy Capacity</b>	231
	P.-H. Lin and E. A. Jorswieck	
9.1	Introduction	231
9.2	Preliminaries	233
	9.2.1 Properties of Wiretap Channels	233
	9.2.2 Properties of Stochastic Orders	234
9.3	System Model	235
9.4	The Relation between Degradedness and Stochastic Orders	236
9.5	The Fast Fading Wiretap Channel with Statistical CSIT	240
	9.5.1 The Layered Erasure Wiretap Channel	240
	9.5.2 The Fast Fading Gaussian Wiretap Channel with Statistical CSIT	242
9.6	Numerical Results	246
9.7	Multiple-Antenna Fading Wiretap Channel with Statistical CSIT	247
	9.7.1 Multiple Antennas without Channel Enhancement	247
	9.7.2 Multiple Antennas with Channel Enhancement	254
9.8	Conclusion	255
	<i>References</i>	256
<b>10</b>	<b>The Discrete Memoryless Arbitrarily Varying Wiretap Channel</b>	258
	J. Nötzel, M. Wiese, and H. Boche	
10.1	Introduction	258
	10.1.1 System Model	258
	10.1.2 Historical Background	260
	10.1.3 New Approaches and New Results	267
10.2	Notation and Definitions	272
	10.2.1 Basic Notation	272
	10.2.2 Models and Operational Definitions	274
10.3	Main Results and Insights	278
	10.3.1 Assisted Capacities: Coding Theorems for $C_{S,\text{ran}}^{\text{mean}}$ , $C_{S,\text{ran}}^{\text{max}}$ , and $C_{\text{key}}$	278
	10.3.2 The Non-Assisted Capacity	280
	10.3.3 Open Questions	287
10.4	Proofs and Intermediate Technical Results	287
	10.4.1 Technical Definitions, Results, and Facts	288
	10.4.2 Basic Quantities and Estimates	290
	10.4.3 Proofs of Lemmas	293
	10.4.4 Proofs of Theorems	295
	<i>References</i>	309

<b>11</b>	<b>Super-Activation as a Unique Feature of Secure Communication over Arbitrarily Varying Channels</b>	313
	R. F. Schaefer, H. Boche, and H. V. Poor	
	11.1 Introduction	313
	11.2 Problem Motivation	315
	11.3 Notation	316
	11.4 Arbitrarily Varying Wiretap Channel	316
	11.4.1 System Model	317
	11.4.2 Code Concepts	319
	11.4.3 Capacity Results	321
	11.5 Super-Activation of Orthogonal AVWCs	322
	11.6 Super-Additivity of Orthogonal AVCs	324
	11.7 Discussion	326
	<i>References</i>	328
<b>Part III</b>	<b>Secret Key Generation and Authentication</b>	331
<b>12</b>	<b>Multiple Secret Key Generation: Information Theoretic Models and Key Capacity Regions</b>	333
	H. Zhang, Y. Liang, L. Lai, and S. Shamai (Shitz)	
	12.1 Introduction	333
	12.2 Hierarchical Model	335
	12.2.1 Model Description	335
	12.2.2 Key Capacity Region	336
	12.3 Cellular Model	340
	12.3.1 Two Key Generation over Three Terminals	340
	12.3.2 Two Key Generation Assisted by a Helper	343
	12.4 Generating Multiple Keys under the PIN Model	352
	12.4.1 Two Pairs Case	353
	12.4.2 General Case	355
	12.5 Discussion and Future Topics	357
	<i>References</i>	359
<b>13</b>	<b>Secret Key Generation for Physical Unclonable Functions</b>	362
	M. Pehl, M. Hiller, and G. Sigl	
	13.1 Introduction	362
	13.2 Notation	364
	13.3 An Information Theoretical View on Key Storage with PUFs	365
	13.3.1 Source Model	365
	13.3.2 Communication Channel	366
	13.3.3 Key Agreement	366
	13.3.4 Rate and Capacity	367
	13.3.5 Attack Vectors	368
	13.3.6 Summary	369

13.4	Unified Algebraic Description of Secret Key and Helper Data Generation	370
13.4.1	Background for Further Analysis	372
13.4.2	Vulnerability of the Pre- and Postprocessing	372
13.4.3	Leakage of the Algebraic Core	374
13.5	Algebraic Core Representations of State-of-the-Art Helper Data Generation	377
13.5.1	Fuzzy Commitment	377
13.5.2	Code-Offset Fuzzy Extractor	378
13.5.3	Fuzzy Extractor with Syndrome Construction	378
13.5.4	Parity Construction	379
13.5.5	Systematic Low Leakage Coding	379
13.5.6	Index-Based Syndrome Coding	380
13.5.7	Complementary IBS	383
13.5.8	Summary of State-of-the-Art Syndrome Decoders	385
13.6	Conclusions	387
	<i>References</i>	387
<b>14</b>	<b>Wireless Physical-Layer Authentication for the Internet of Things</b>	<b>390</b>
	G. Caparra et al.	
14.1	IoT Authentication Overview	390
14.2	State of the Art	392
14.2.1	Physical-Layer Authentication	393
14.3	IoT Channel-Based Authentication	395
14.3.1	Authentication Protocol	396
14.3.2	Authentication Protocol Performance	399
14.4	Centralized Anchor Node Selection	402
14.4.1	Energy-Efficient Anchor Node Selection	404
14.4.2	Signaling-Efficient Anchor Selection	405
14.4.3	A Tradeoff between Energy Efficiency and Signaling Efficiency	407
14.5	Distributed Anchor Node Selection	410
14.5.1	Distributed Configuration Selection	410
14.5.2	Distributed SNR-Based Anchor Node Selection	411
14.6	Performance Summary and Conclusions	414
14.6.1	Summary	414
	<i>References</i>	415
<b>Part IV</b>	<b>Data Systems and Related Applications</b>	<b>419</b>
<b>15</b>	<b>Information Theoretic Analysis of the Performance of Biometric Authentication Systems</b>	<b>421</b>
	T. Ignatenko and F. M. J. Willems	
15.1	Introduction	421
15.1.1	Chapter Organization	423

15.2	Enrollment and Authentication Statistics	423
15.3	Traditional Authentication Systems	424
15.3.1	Scenario and Objective	424
15.3.2	Achievability Definition and Result	424
15.3.3	Discussion	426
15.4	Rate-Constrained Authentication Systems	427
15.4.1	Scenario and Objective	427
15.4.2	Achievability Definition and Result	427
15.4.3	Discussion	429
15.5	Secret-Key-Based Authentication Systems	430
15.5.1	Scenario and Objective	430
15.5.2	System Building Blocks: Encoder, Decoder, and Equality Checker; FRR and mFAR	430
15.5.3	Definition of Achievability and Statement of Result	431
15.5.4	Relation to Ahlswede–Csiszár Secret Generation	431
15.5.5	Discussion	434
15.6	Proof of Theorem 15.3	434
15.6.1	Achievability Proof for Theorem 15.3	434
15.6.2	Converse for Theorem 15.3	437
15.7	Privacy Leakage in Secret-Based Systems	439
15.8	Proof of Theorem 15.5	439
15.8.1	Achievability Part for Theorem 15.5	440
15.8.2	Converse for Theorem 15.5	442
15.9	Conclusions and Final Remarks	443
	<i>References</i>	443
<b>16</b>	<b>Joint Privacy and Security of Multiple Biometric Systems</b>	<b>445</b>
	A. Goldberg and S. C. Draper	
16.1	Introduction	445
16.1.1	Biometric System Design Requirements	446
16.1.2	Security and Privacy Leakage	447
16.1.3	Related Work	450
16.2	Problem Formulation	451
16.3	Design Space	455
16.3.1	Geometric Intuition	457
16.3.2	Scaling Complexity	460
16.3.3	Equivalent Designs	461
16.4	The Fixed-Basis Case	462
16.4.1	Impact of the Restriction	462
16.4.2	Optimization of Fixed-Basis Designs	463
16.4.3	Resulting Privacy/Security Tradeoff	469
16.4.4	Observed Form of Optimal Solutions	470
16.5	Conclusions	471
	<i>References</i>	471



<b>17</b>	<b>Information Theoretic Approaches to Privacy-Preserving Information Access and Dissemination</b>	473
	G. Fanti and K. Ramchandran	
	17.1 Introduction	473
	17.2 Information Dissemination	475
	17.2.1 Anonymous Broadcast Messaging	476
	17.2.2 Anonymous Point-to-Point Messaging	482
	17.3 Information Access	483
	17.3.1 Adversarial Models	484
	17.3.2 Private Information Retrieval	485
	17.3.3 Private Streaming Search	491
	17.3.4 Encrypted Databases	493
	17.4 Conclusions	493
	<i>References</i>	494
<b>18</b>	<b>Privacy in the Smart Grid: Information, Control, and Games</b>	499
	H. V. Poor	
	18.1 Introduction	499
	18.2 Information: A General Formalism	500
	18.3 Control: Smart Meter Privacy	504
	18.4 Games: Competitive Privacy	510
	18.5 Conclusion	515
	<i>References</i>	516
<b>19</b>	<b>Security in Distributed Storage Systems</b>	519
	S. El Rouayheb, S. Goparaju, and K. Ramchandran	
	19.1 Introduction	519
	19.1.1 Related Literature	521
	19.1.2 Organization	522
	19.2 Model and Notation	522
	19.2.1 System Model	522
	19.2.2 Security and Adversary Model	524
	19.2.3 Secrecy Capacity and Notation	524
	19.2.4 Flow Graph Representation	526
	19.3 Secrecy against Passive Eavesdropping	526
	19.3.1 Upper Bound on the Secrecy Capacity	527
	19.3.2 Achievability of the Secrecy Capacity	528
	19.3.3 Secrecy via Separation Schemes	531
	19.3.4 Separation Secrecy Capacity of Linear Optimal Repair MDS Codes	533
	19.3.5 Universally Secure Optimal Repair MDS Codes	537
	19.4 Security against an Omniscient Adversary	537
	19.4.1 Upper Bound on the Resiliency Capacity	538
	19.4.2 Achievability of the Resiliency Capacity Upper Bound	539

19.5	Security against a Limited-Knowledge Adversary	541
19.5.1	Resiliency Capacity	542
19.5.2	Secure Scheme Example	542
19.5.3	Proof of Theorem 19.9	545
19.6	Conclusion and Open Problems	547
	<i>References</i>	548
	<i>Index</i>	554