## Information Theoretic Security and Privacy of Information Systems

Gain a solid understanding of how information theoretic approaches can inform the design of more secure information systems and networks with this authoritative text. With a particular focus on theoretical models and analytical results, leading researchers show how techniques derived from the principles of source and channel coding can provide new ways of addressing issues of data security, embedded security, privacy, and authentication in modern information systems. A wide range of wireless and cyber-physical systems is considered, including 5G cellular networks, the Tactile Internet, biometric identification systems, online data repositories, and smart electricity grids. This is an invaluable guide for both researchers and graduate students working in communications engineering, and industry practitioners and regulators interested in improving security in the next generation of information systems.

**Rafael F. Schaefer** is an Assistant Professor at the Technische Universität Berlin, having previously worked at Princeton University.

**Holger Boche** is a Full Professor at the Technische Universität München, a member of the German Academy of Sciences, and a Fellow of the IEEE. He is also a co-editor of *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2013).

**Ashish Khisti** is an Associate Professor and a Canada Research Chair in the Department of Electrical and Computer Engineering at the University of Toronto.

**H. Vincent Poor** is the Michael Henry Strater University Professor at Princeton University, a member of the US National Academies of Engineering and Sciences, and a Fellow of the IEEE. He has co-authored and co-edited several books, including *Quickest Detection* (Cambridge University Press, 2008) and *Smart Grid Communications and Networking* (Cambridge University Press, 2012).

# Information Theoretic Security and Privacy of Information Systems

RAFAEL F. SCHAEFER
Technische Universität Berlin

HOLGER BOCHE
Technische Universität München

ASHISH KHISTI
University of Toronto

H. VINCENT POOR
Princeton University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi – 110002, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107132269
10.1017/9781316450840



First published 2017

Printed in the United Kingdom by Clays, St Ives plc

*A catalogue record for this publication is available from the British Library*

ISBN 978-1-107-13226-9 Hardback

# Contents

*List of Contributors* *page* xv
*Preface* xix

**Part I Theoretical Foundations** 1

**1 Effective Secrecy: Reliability, Confusion, and Stealth** 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
*References* 19

**2 Error-Free Perfect Secrecy Systems** 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
*References* 50

**3 Secure Source Coding** 51
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
*References* 75

**4 Networked Secure Source Coding** 77
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
*References* 104

**Part II Secure Communication** 107

**5 Secrecy Rate Maximization in Gaussian MIMO Wiretap Channels** 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
*References* 137

**6 MIMO Wiretap Channels** 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
*References* 178

**7 MISO Wiretap Channel with Strictly Causal CSI: A Topological Viewpoint** 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
*References* 197

**8 Physical-Layer Security with Delayed, Hybrid, and Alternating Channel State Knowledge** 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
*References* 226

**9 Stochastic Orders, Alignments, and Ergodic Secrecy Capacity** 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
*References* 256

**10 The Discrete Memoryless Arbitrarily Varying Wiretap Channel** 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 $C_{\mathrm{S,ran}}^{\mathrm{mean}}$, $C_{\mathrm{S,ran}}^{\mathrm{max}}$, and $C_{\mathrm{key}}$ 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
*References* 309

**11 Super-Activation as a Unique Feature of Secure Communication over Arbitrarily Varying Channels** 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
*References* 328

**Part III Secret Key Generation and Authentication** 331

**12 Multiple Secret Key Generation: Information Theoretic Models and Key Capacity Regions** 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
*References* 359

**13 Secret Key Generation for Physical Unclonable Functions** 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
*References* 387

**14 Wireless Physical-Layer Authentication for the Internet of Things** 390
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
*References* 415

**Part IV Data Systems and Related Applications** 419

**15 Information Theoretic Analysis of the Performance of Biometric Authentication Systems** 421
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
*References* 443

**16 Joint Privacy and Security of Multiple Biometric Systems** 445
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
*References* 471

**17 Information Theoretic Approaches to Privacy-Preserving Information Access and Dissemination** 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
*References* 494

**18 Privacy in the Smart Grid: Information, Control, and Games** 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
*References* 516

**19 Security in Distributed Storage Systems** 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
*References* 548

*Index* 554

# Contributors

**Zohaib Hassan Awan**
Lehrstuhl für Digitale Kommunikationssysteme, Ruhr-Universität Bochum

**Matthieu Bloch**
School of Electrical and Computer Engineering, Georgia Institute of Technology

**Holger Boche**
Chair of Theoretical Information Technology, Technische Universität München

**Gianluca Caparra**
Department of Information Engineering, University of Padova

**Marco Centenaro**
Department of Information Engineering, University of Padova

**Terence Chan**
Institute for Telecommunications Research, University of South Australia

**Charalambos D. Charalambous**
Department of Electrical and Computer Engineering, University of Cyprus

**Paul Cuff**
Department of Electrical Engineering, Princeton University

**Stark C. Draper**
Department of Electrical and Computer Engineering, University of Toronto

**Salim El Rouayheb**
Department of Electrical and Computer Engineering, Illinois Institute of Technology

**Giulia Fanti**
Department of Electrical Engineering and Computer Science, University of California, Berkeley

**Adina Goldberg**
Department of Electrical and Computer Engineering, University of Toronto

**Sreechakra Goparaju**
Qualcomm Institute, University of California, San Diego

**Alex Grant**
Myriota, Adelaide, Australia

**Matthias Hiller**
Fraunhofer Institute for Applied and Integrated Security

**Siu-Wai Ho**
Institute for Telecommunications Research, University of South Australia

**Jie Hou**
European Patent Office Munich

**Tanya Ignatenko**
Electrical Engineering Department, Eindhoven University of Technology

**Eduard A. Jorswieck**
Chair for Communications Theory, Technische Universität Dresden

**Kittipong Kittichokechai**
Communications and Information Theory Chair, Technische Universität Berlin

**Gerhard Kramer**
Chair of Communications Engineering, Technische Universität München

**Lifeng Lai**
Department of Electrical and Computer Engineering, University of California, Davis

**Nicola Laurenti**
Department of Information Engineering, University of Padova

**Yingbin Liang**
Department of Electrical Engineering and Computer Science, Syracuse University

**Pin-Hsun Lin**
Chair for Communications Theory, Technische Universität Dresden

**Sergey Loyka**
School of Electrical Engineering and Computer Science, University of Ottawa

**Pritam Mukherjee**
Department of Electrical and Computer Engineering, University of Maryland

**Mohamed Nafea**
Wireless Communications and Networking Laboratory (WCAN), Electrical Engineering Department, The Pennsylvania State University

**Janis Nötzel**
Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona

**Tobias J. Oechtering**
Information Science and Engineering Department, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology

**Michael Pehl**
Chair of Security in Information Technology, Technische Universität München

**H. Vincent Poor**
Department of Electrical Engineering, Princeton University

**Kannan Ramchandran**
Department of Electrical Engineering and Computer Science, University of California, Berkeley

**Rafael F. Schaefer**
Information Theory and Applications Chair, Technische Universität Berlin

**Curt Schieler**
Lincoln Laboratory, Massachusetts Institute of Technology

**Aydin Sezgin**
Lehrstuhl für Digitale Kommunikationssysteme, Ruhr-Universität Bochum

**Shlomo Shamai (Shitz)**
Department of Electrical Engineering, Technion-Israel Institute of Technology

**Georg Sigl**
Chair of Security in Information Technology, Technische Universität München
and
Fraunhofer Institute for Applied and Integrated Security

**Mikael Skoglund**
Information Science and Engineering Department, School of Electrical Engineering and ACCESS Linnaeus Center, KTH Royal Institute of Technology

**Ravi Tandon**
Department of Electrical and Computer Engineering, University of Arizona

**Stefano Tomasin**
Department of Information Engineering, University of Padova

**Chinthani Uduwerelle**
Institute for Telecommunications Research, University of South Australia

**Sennur Ulukus**
Department of Electrical and Computer Engineering, University of Maryland

**Lorenzo Vangelista**
Department of Information Engineering, University of Padova

**Moritz Wiese**
ACCESS Linnaeus Center and Automatic Control Lab, School of Electrical Engineering, KTH Royal Institute of Technology

**Frans M. J. Willems**
Electrical Engineering Department, Eindhoven University of Technology

**Aylin Yener**
Wireless Communications and Networking Laboratory (WCAN), Electrical Engineering Department, The Pennsylvania State University

**Huishuai Zhang**
Department of Electrical Engineering and Computer Science, Syracuse University

# Preface

The ubiquity of information technologies such as wireless communications, biometric identification systems, online data repositories, and smart electricity grids has created new challenges in information security and privacy. Traditional approaches based on cryptography are often inadequate in such complex systems and fundamentally new techniques must be developed. Information theory provides fundamental limits that can guide the development of methods for addressing these challenges, and the purpose of this book is to introduce the reader to state-of-the-art developments in this field.

As a prototypical example of a system in which such methods can play an important role, one can consider a communication system. In a typical configuration, there is an architectural separation between data encryption and error correction in such systems. The encryption module is based on cryptographic principles and abstracts out the underlying communication channel as an ideal bit-pipe. The error correction module is typically implemented at the physical layer. It adds redundancy into the source message in order to combat channel impairments or multiuser interference and transforms the noisy communication channel into a reliable bit-pipe. While such a separation-based architecture has long been an obvious solution in most systems, a number of applications have emerged in recent years where encryption mechanisms must be aware of the noise structure in the underlying channel, and likewise the error correction and data compression methods must be aware of the associated secrecy constraints required by the application. Such joint approaches can be studied by developing new mathematical models of communication systems that impose both reliability constraints and secrecy constraints. Similar considerations arise throughout the information and communication technologies, and information theoretic approaches can point the way to fundamentally new solutions for such technologies. We refer to this emerging field of research as *information theoretic approaches to security and privacy* (ITASP). It is notable that this approach leads to guaranteeing information security irrespective of the computational power of the adversary and is a fundamental departure from current computation-based cryptographic solutions. In this book we will highlight among others the following application areas where principles of ITASP have been particularly effective.

**Wireless systems:** Mobile links are traditionally considered to be the weakest links in network security. The current separation-based architectures allow for a variety of attacks that exploit the broadcast nature of wireless links. Fortunately, when we consider ITASP, a number of new solutions emerge that have been traditionally overlooked by

the separation-based architecture. In fact, for ITASP, the broadcast nature of wireless links turns out to be a strength, allowing for new methods of secret key generation, as well as key-less confidential data transmission, to be developed. Physical layer design of wireless systems has dramatically advanced in the last decade to support the growing demands from end users effectively utilizing cooperative relays, multiple-antenna arrays, and channel adaptation strategies, and these advances are making their way into reality. Moreover, emerging concepts such as the Internet of Things introduce network architectural and scaling issues that make traditional methods of providing information security impractical. It is only natural that we now can envision that the physical-layer-based approaches rooted in ITASP can significantly enhance the security and privacy of wireless networks in the near future.

**Biometric systems:** Biometrics such as fingerprints, iris scan, etc. provide the most compelling means of authentication as they directly use the physical attributes of a user. Surprisingly, practical systems suffer from a serious privacy concern. Many of the commercially available systems store the biometric reading measured during the enrollment phase in the clear. This is because successive biometric readings of the same user are somewhat different due to measurement noise. Thus the one-way hash functions widely used when storing passwords cannot be used in such systems. Interestingly, it has been recently recognized that a class of secure hash functions that are robust to measurement noise can be implemented in such systems. The principles of such robust hash functions are intimately tied to a well-studied problem in ITASP, i.e., the "source model" in secret key generation.

**Smart-grid systems:** There has been a strong push toward modernizing the electric power grid in most developed countries, using advanced metering infrastructure (AMI) and sensors within the grid. Privacy and security concerns are a major issue in the design and deployment of such systems. For example, AMI systems report real-time measurements of the electricity consumption of each individual household. While such information can be vital for load balancing, it also raises serious privacy concerns, as end-user behavior can be easily inferred from the instantaneous electricity usage. Thus a fundamental tradeoff between utility and privacy exists in such systems, and the ITASP framework is a natural way of characterizing such a tradeoff.

This book provides scientific insights into the emerging field of ITASP. Presenting contributions from prominent researchers in this area, the book not only gives an overview of state-of-the-art research results but also builds a strong foundation for designing future systems incorporating ITASP. The book is organized in four parts: (I) theoretical foundations; (II) secure communication; (III) secret key generation and authentication; and (IV) data systems and related applications. The first part focuses on fundamental concepts of information theoretic security in general. The second part of the book focuses on secure communication. These range from multiple-input multiple-output wiretap channels to different concepts of imperfect channel state information and its implications. The third part discusses secret key generation and authentication over the wireless channel. And finally, the fourth part focuses on data systems and related applications such as biometric authentication, smart grid, and distributed storage systems.

While this treatment primarily adopts an analytical approach, implications of theoretical results and associated insights are discussed explicitly. Often the study of relatively simple information theoretic models can lead to surprising insights that can fundamentally change the way we approach the design of security mechanisms. Thus a significant number of chapters presented in this book are devoted to the study of such models. With a modern presentation style, the book aims to go beyond a dry recapture of published theoretical results and reach a broader audience by providing insights to the consequences of technological and theoretical developments. The reader will also benefit from diverse perspectives on the underlying issues brought to the book by multiple prominent contributing authors.

This treatment is suitable for graduate students and other researchers who wish to gain an entrée into this field, or to expand their existing knowledge of it. It can serve, for example, as the basis for an advanced graduate course in ITASP. It is also of interest to practicing engineers and computer scientists working in communications and information technology who wish to gain an understanding of the possibilities of this emerging field.