Physical-Layer Security
From Information Theory to Security Engineering

This complete guide to physical-layer security presents the theoretical foundations, practical implementation, challenges, and benefits of a groundbreaking new model for secure communication. Using a bottom-up approach from the link level all the way to end-to-end architectures, it provides essential practical tools that enable graduate students, industry professionals, and researchers to build more secure systems by exploiting the noise inherent to communication channels.

The book begins with a self-contained explanation of the information-theoretic limits of secure communications at the physical layer. It then goes on to develop practical coding schemes, building on the theoretical insights and enabling readers to understand the challenges and opportunities related to the design of physical-layer security schemes. Finally, applications to multi-user communications and network coding are also included.

Matthieu Bloch is an Assistant Professor in the School of Electrical Engineering of the Georgia Institute of Technology. He received a Ph.D. in Engineering Science from the Université de Franche-Comté, Besançon, France, in 2006, and a Ph.D. in Electrical Engineering from the Georgia Institute of Technology in 2008. His research interests are in the areas of information theory, error-control coding, wireless communications, and quantum cryptography.

João Barros is an Associate Professor in the Department of Electrical and Computer Engineering of the Faculdade de Engenharia da Universidade do Porto, the Head of the Porto Delegation of the Instituto de Telecomunicações, Portugal, and a Visiting Professor at the Massachusetts Institute of Technology. He received his Ph.D. in Electrical Engineering and Information Technology from the Technische Universität München (TUM), Germany, in 2004 and has since published extensively in the general areas of information theory, communication networks, and security. He has taught short courses and tutorials at various institutions and received a Best Teaching Award from the Bavarian State Ministry of Sciences and the Arts, as well as the 2010 IEEE ComSoc Young Researcher Award for Europe, the Middle East, and Africa.
Physical-Layer Security

From Information Theory to Security Engineering

MATTHIEU BLOCH
Georgia Institute of Technology

JOÃO BARROS
University of Porto
To our families
Contents

Preface xi
Notation xiii
List of abbreviations xv

Part I Preliminaries

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

### 3 Secrecy capacity

3.1 Shannon’s cipher system  
3.2 Secure communication over a noisy channel  
3.3 Perfect, weak, and strong secrecy  
3.4 Wyner’s wiretap channel  
  3.4.1 Achievability proof for the degraded wiretap channel  
  3.4.2 Converse proof for the degraded wiretap channel  
3.5 Broadcast channel with confidential messages  
  3.5.1 Channel comparison  
  3.5.2 Achievability proof for the broadcast channel with confidential messages  
  3.5.3 Converse proof for the broadcast channel with confidential messages  
3.6 Multiplexing and feedback  
  3.6.1 Multiplexing secure and non-secure messages  
  3.6.2 Feedback and secrecy  
3.7 Conclusions and lessons learned  
3.8 Bibliographical notes

### 4 Secret-key capacity

4.1 Source and channel models for secret-key agreement  
4.2 Secret-key capacity of the source model  
  4.2.1 Secret-key distillation based on wiretap codes  
  4.2.2 Secret-key distillation based on Slepian–Wolf codes  
  4.2.3 Upper bound for secret-key capacity  
  4.2.4 Alternative upper bounds for secret-key capacity  
4.3 Sequential key distillation for the source model  
  4.3.1 Advantage distillation  
  4.3.2 Information reconciliation  
  4.3.3 Privacy amplification  
4.4 Secret-key capacity of the channel model  
4.5 Strong secrecy from weak secrecy  
4.6 Conclusions and lessons learned  
4.7 Appendix  
4.8 Bibliographical notes

### 5 Security limits of Gaussian and wireless channels

5.1 Gaussian channels and sources  
  5.1.1 Gaussian broadcast channel with confidential messages  
  5.1.2 Multiple-input multiple-output Gaussian wiretap channel  
  5.1.3 Gaussian source model  
5.2 Multiple-access Gaussian channel with confidential messages  
5.3 Multi-hop Gaussian wiretap channel  
5.4 Gaussian relay channel  
5.5 Gaussian interference channel  
5.6 Conclusions and lessons learned  
5.7 Bibliographical notes
Contents

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

References 311
Author index 323
Subject index 326
Preface

This book is the result of more than five years of intensive research in collaboration with a large number of people. Since the beginning, our goal has been to understand at a deeper level how information-theoretic security ideas can help build more secure networks and communication systems. Back in 2008, the actual plan was to finish the manuscript within one year, which for some reason seemed a fairly reasonable proposition at that time. Needless to say, we were thoroughly mistaken. The pace at which physical-layer security topics have found their way into the main journals and conferences in communications and information theory is simply staggering. In fact, there is now a vibrant scientific community uncovering the benefits of looking at the physical layer from a security point of view and producing new results every day. Writing a book on physical-layer security thus felt like shooting at not one but multiple moving targets.

To preserve our sanity we decided to go back to basics and focus on how to bridge the gap between theory and practice. It did not take long to realize that the book would have to appeal simultaneously to information theorists, cryptographers, and network-security specialists. More precisely, the material could and should provide a common ground for fruitful interactions between those who speak the language of security and those who for a very long time focused mostly on the challenges of communicating over noisy channels. Therefore, we opted for a mathematical treatment that addresses the fundamental aspects of information-theoretic security, while providing enough background on cryptographic protocols to allow an eclectic and synergistic approach to the design of security systems.

The book is intended for several different groups: (a) communication engineers and security specialists who wish to understand the fundamentals of physical-layer security and apply them in the development of real-life systems, (b) scientists who aim at creating new knowledge in information-theoretic security and applications, (c) graduate students who wish to be trained in the fundamental techniques, and (d) decision makers who seek to evaluate the potential benefits of physical-layer security. If this book leads to many exciting discussions at the white board among diverse groups of people, then our goal will have been achieved.

Finally, we would like to acknowledge all our colleagues, students, and friends who encouraged us and supported us during the course of this project. First and foremost, we are deeply grateful to Steve McLaughlin, who initiated the project and let us run with it. Special thanks are also due to Phil Meyer and Sarah Matthews from Cambridge University Press for their endless patience as we postponed the delivery of the manuscript countless times. We express our sincere gratitude to Demijan Klinc and Alexandre
Preface

Pierrot, who proofread the entire book in detail many times and relentlessly asked for clarification, simplification, and consistent notation. We would like to thank Glenn Bradford, Michael Dickens, Brian Dunn, Jing Huang, Utsaw Kumar, Ebrahim Molavian-Jazi, and Zhanwei Sun for attending EE 87023 at the University of Notre Dame when the book was still a set of immature lecture notes. The organization and presentation of the book have greatly benefited from their candid comments. Thanks are also due to Nick Laneman, who provided invaluable support. Willie Harrison, Xiang He, Mari Kobayashi, Ashish Khisti, Francesco Renna, Osvaldo Simeone, Andrew Thangaraj, and Aylin Yener offered very constructive comments. The book also benefited greatly from many discussions with Prakash Narayan, Imre Csiszár, Muriel Médard, Ralf Koetter, and Pedro Pinto, who generously shared their knowledge with us. Insights from research by Miguel Rodrigues, Luísa Lima, João Paulo Vilela, Paulo Oliveira, Gerhard Maierbacher, Tiago Vinhoza, and João Almeida at the University of Porto also helped shape the views expressed in this volume.

Matthieu Bloch, Georgia Institute of Technology
João Barros, University of Porto
## Notation

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GF(q)</td>
<td>Galois field with q elements</td>
</tr>
<tr>
<td>ℜ</td>
<td>field of real numbers</td>
</tr>
<tr>
<td>ℂ</td>
<td>field of complex numbers</td>
</tr>
<tr>
<td>ℤ</td>
<td>set of natural numbers (ℤ+ excludes 0)</td>
</tr>
<tr>
<td>℧</td>
<td>alphabet or set</td>
</tr>
<tr>
<td>℧</td>
<td>cardinality of ℧</td>
</tr>
<tr>
<td>cl(℧)</td>
<td>closure of set ℧</td>
</tr>
<tr>
<td>co(℧)</td>
<td>convex hull of set ℧</td>
</tr>
<tr>
<td>⊙</td>
<td>indicator function</td>
</tr>
<tr>
<td>℧₁</td>
<td>sequence x₁, …, xₙ</td>
</tr>
<tr>
<td></td>
<td>sequence with n repetitions of the same element x</td>
</tr>
<tr>
<td>ε</td>
<td>usually, a “small” positive real number</td>
</tr>
<tr>
<td>δ(ε)</td>
<td>a function of ε such that ( \lim_{ε \to 0} δ(ε) = 0 )</td>
</tr>
<tr>
<td>δ₁(n)</td>
<td>a function of ε and n such that ( \lim_{n \to ∞} δ₁(n) = 0 )</td>
</tr>
<tr>
<td>δ(n)</td>
<td>a function of n such that ( \lim_{n \to ∞} δ(n) = 0 )</td>
</tr>
<tr>
<td>x</td>
<td>column vector containing the n elements x₁, x₂, …, xₙ</td>
</tr>
<tr>
<td>xᵀ</td>
<td>transpose of x</td>
</tr>
<tr>
<td>x†</td>
<td>Hermitian transpose of x</td>
</tr>
<tr>
<td>H</td>
<td>matrix</td>
</tr>
<tr>
<td>(hᵢⱼ)ₘ,ₙ</td>
<td>m × n matrix whose elements are hᵢⱼ, with i ∈ [1, m] and j ∈ [1, n]</td>
</tr>
<tr>
<td></td>
<td>determinant of matrix H</td>
</tr>
<tr>
<td>tr(H)</td>
<td>trace of matrix H</td>
</tr>
<tr>
<td>rk(H)</td>
<td>rank of matrix H</td>
</tr>
<tr>
<td>Ker(H)</td>
<td>kernel of matrix H</td>
</tr>
</tbody>
</table>
xiv  Notation

X random variable implicitly defined on alphabet X
\( p_X \) probability distribution of random variable X
\( X \sim p_X \) random variable X with distribution \( p_X \)
\( \mathcal{N}(\mu, \sigma^2) \) Gaussian distribution with mean \( \mu \) and variance \( \sigma^2 \)
\( B(p) \) Bernoulli distribution with parameter \( p \)
\( p_{X|Y} \) conditional probability distribution of X given Y
\( T^n(X) \) strong typical set with respect to \( p_X \)
\( T^n(XY) \) strong joint-typical set with respect to \( p_{XY} \)
\( T^n(X|X^n) \) conditional strong typical set with respect to \( p_{XY} \) and \( x^n \)
\( A^n(x) \) weak typical set with respect to \( p_X \)
\( A^n(XY) \) joint weak typical set with respect to \( p_{XY} \)
\( E_X \) expected value over random variable X
\( Var(X) \) variance of random variable X
\( \Pr[X] \) probability of an event over X
\( H(X) \) Shannon entropy of discrete random variable X
\( H_b \) binary entropy function
\( H_c(X) \) collision entropy of discrete random variable X
\( H_\infty(X) \) min-entropy of discrete random variable X
\( h(X) \) differential entropy of continuous random variable X
\( I(X;Y) \) mutual information between random variables X and Y
\( P_e(C) \) probability of error of a code C
\( E(C) \) equivocation of a code C
\( L(C) \) information leakage of a code C
\( U(S) \) uniformity of keys guaranteed by key-distillation strategy S
\( \lim_{x \to c} f(x) \) limit inferior of \( f(x) \) as \( x \) goes to \( c \)
\( \lim_{x \to c} f(x) \) limit superior of \( f(x) \) as \( x \) goes to \( c \)
\( f(x) = O(g(x)) \) If \( g \) is non-zero for large enough values of \( x \),
\( f(x) = O(g(x)) \) as \( x \to a \) if and only if
\( \lim_{x \to \infty} |f(x)/g(x)| < \infty. \)
Abbreviations

AES       Advanced Encryption Standard
AWGN      additive white Gaussian noise
BC        broadcast channel
BCC       broadcast channel with confidential messages
BEC       binary erasure channel
BSC       binary symmetric channel
CA        certification authority
DES       Data Encryption Standard
DMC       discrete memoryless channel
DMS       discrete memoryless source
DSRC      Dedicated Short-Range Communication
DSS       direct sequence spreading
DWTC      degraded wiretap channel
EAP       Extensible Authentication Protocol
EPC       Electronic Product Code
ESP       Encapsulating Security Payload
FH        frequency hopping
GPRS      General Packet Radio Service
GSM       Global System for Mobile Communications
IETF      Internet Engineering Task Force
IP        Internet Protocol
LDPC      low-density parity-check
LLC       logical link control
LLR       log-likelihood ratio
LPI       low probability of intercept
LS        least square
LTE       Long Term Evolution
MAC       multiple-access channel
MIMO      multiple-input multiple-output
NFC       near-field communication
NIST      National Institute of Standards and Technology, USA
OSI       open system interconnection
PKI       public key infrastructure
RFID      radio-frequency identification
## List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>Rivest–Shamir–Adleman</td>
</tr>
<tr>
<td>SIM</td>
<td>subscriber identity module</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TDD</td>
<td>time-division duplex</td>
</tr>
<tr>
<td>TLS</td>
<td>transport layer security</td>
</tr>
<tr>
<td>TWWTC</td>
<td>two-way wiretap channel</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>WTC</td>
<td>Wiretap channel</td>
</tr>
<tr>
<td>XOR</td>
<td>exclusive OR</td>
</tr>
</tbody>
</table>