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.

Cambridge University Press
978-0-521-51650-1 - Physical-Layer Security: From Information Theory to Security Engineering
Matthieu Bloch and João Barros
Frontmatter
More information

Physical-Layer Security

From Information Theory to Security Engineering

MATTHIEU BLOCH
Georgia Institute of Technology

JOÃO BARROS
University of Porto

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521516501

First published 2011

Printed in the United Kingdom at the University Press, Cambridge

A catalog record for this publication is available from the British Library

ISBN 978-0-521-51650-1 Hardback

To our families

Contents

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

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

$\mathrm{GF}(q)$	Galois field with q elements
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$\mathbb{N}$	set of natural numbers ($\mathbb{N}^*$ excludes 0)
$\mathcal{X}$	alphabet or set
$\lvert\mathcal{X}\rvert$	cardinality of $\mathcal{X}$
$\mathrm{cl}(\mathcal{X})$	closure of set $\mathcal{X}$
$\mathrm{co}(\mathcal{X})$	convex hull of set $\mathcal{X}$
$\mathbb{1}$	indicator function
$\{x_i\}_n$	ensemble with n elements $\{x_1, \dots, x_n\}$
x	generic element of alphabet $\mathcal{X}$
$\lvert x\rvert$	absolute value of x
$\lceil x\rceil$	unique integer n such that $x \leqslant n < x + 1$
$\lfloor x\rfloor$	unique integer n such that $x - 1 \leqslant n \leqslant x$
$[\![x, y]\!]$	sequence of integers between $\lfloor x\rfloor$ and $\lceil y\rceil$
x^+	positive part of x, that is $x^+ = \max(x, 0)$
$\mathrm{sign}(x)$	$+1$ if $x \geqslant 0$, -1 otherwise
x^n	sequence $x_1, \dots, x_n$
$\bar{x}^n$	sequence with n repetitions of the same element x
ϵ	usually, a “small” positive real number
$\delta(\epsilon)$	a function of ϵ such that $\lim_{\epsilon\to 0} \delta(\epsilon) = 0$
$\delta_\epsilon(n)$	a function of ϵ and n such that $\lim_{n\to\infty} \delta_\epsilon(n) = 0$
$\delta(n)$	a function of n such that $\lim_{n\to\infty} \delta(n) = 0$
$\mathbf{x}$	column vector containing the n elements $x_1, x_2, \dots, x_n$
$\mathbf{x}^\mathsf{T}$	transpose of $\mathbf{x}$
$\mathbf{x}^\dagger$	Hermitian transpose of $\mathbf{x}$
$\mathbf{H}$	matrix
$(h_{ij})_{m,n}$	$m \times n$ matrix whose elements are h_{ij}, with $i \in [\![1, m]\!]$ and $j \in [\![1, n]\!]$
$\lvert\mathbf{H}\rvert$	determinant of matrix $\mathbf{H}$
$\mathrm{tr}(\mathbf{H})$	trace of matrix $\mathbf{H}$
$\mathrm{rk}(\mathbf{H})$	rank of matrix $\mathbf{H}$
$\mathrm{Ker}(\mathbf{H})$	kernel of matrix $\mathbf{H}$

X	random variable implicitly defined on alphabet $\mathcal{X}$
p_{X}	probability distribution of random variable X
$\mathsf{X} \sim p_{\mathsf{X}}$	random variable X with distribution p_{X}
$\mathcal{N}(\mu, \sigma^2)$	Gaussian distribution with mean μ and variance σ^2
$\mathcal{B}(p)$	Bernoulli distribution with parameter p
$p_{\mathsf{X}\vert\mathsf{Y}}$	conditional probability distribution of X given Y
$\mathcal{T}_\epsilon^n(\mathsf{X})$	strong typical set with respect to p_{X}
$\mathcal{T}_\epsilon^n(\mathsf{XY})$	strong joint-typical set with respect to p_{XY}
$\mathcal{T}_\epsilon^n(\mathsf{XY}\vert x^n)$	conditional strong typical set with respect to p_{XY} and x^n
$\mathcal{A}_\epsilon^n(\mathsf{X})$	weak typical set with respect to p_{X}
$\mathcal{A}_\epsilon^n(\mathsf{XY})$	joint weak typical set with respect to p_{XY}
$\mathbb{E}_{\mathsf{X}}$	expected value over random variable X
$\mathrm{Var}(\mathsf{X})$	variance of random variable X
$\mathbb{P}_{\mathsf{X}}$	probability of an event over X
$\mathbb{H}(\mathsf{X})$	Shannon entropy of discrete random variable X
$\mathbb{H}_b$	binary entropy function
$\mathbb{H}_c(\mathsf{X})$	collision entropy of discrete random variable X
$\mathbb{H}_\infty(\mathsf{X})$	min-entropy of discrete random variable X
$\mathbb{h}(\mathsf{X})$	differential entropy of continuous random variable X
$\mathbb{I}(\mathsf{X};\mathsf{Y})$	mutual information between random variables X and Y
$\mathbf{P}_e(\mathcal{C})$	probability of error of a code $\mathcal{C}$
$\mathbf{E}(\mathcal{C})$	equivocation of a code $\mathcal{C}$
$\mathbf{L}(\mathcal{C})$	information leakage of a code $\mathcal{C}$
$\mathbf{U}(\mathcal{S})$	uniformity of keys guaranteed by key-distillation strategy $\mathcal{S}$
$\underline{\lim}_{x\to c} f(x)$	limit inferior of $f(x)$ as x goes to c
$\overline{\lim}_{x\to c} f(x)$	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 $\overline{\lim}_{x\to\infty} \lvert f(x)/g(x)\rvert < \infty$.

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

RSA	Rivest–Shamir–Adleman
SIM	subscriber identity module
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDD	time-division duplex
TLS	transport layer security
TWWTC	two-way wiretap channel
UMTS	Universal Mobile Telecommunication System
WTC	Wiretap channel
XOR	exclusive OR