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