Review of the book

"Foundations of Cryptography"

by Oded Goldreich
Cambridge University Press, 2001 and 2004

ISBN: 978-0-521-79172-3 and 978-0-521-83084-2

Edoardo Persichetti
University of Warsaw
May 2013

1 Summary of the review

In this review I present "Foundations of Cryptography" by Oded Goldreich. This two-volume work gives an extensive description of the theoretical foundations of modern cryptography. It is beneficial to keep in mind that the two volumes are two parts of a whole, and in particular the second volume builds heavily on the first.

2 Summary of the book

Modern cryptography is a very vast and inter-disciplinar subject. It combines elements from mathematics, computer science, and engineering, with the aim of designing systems for secure communication. Very rigorous and formal foundations are required to properly describe all the issues which concern cryptography; this book seeks to give a detailed treatment of all these foundations, presenting the most important tools and applications as building blocks for solving cryptographic problems.
The book is divided into two volumes: the first volume features all the basic tools that are necessary to define and approach the subject. In the second volume are instead described the main applications such as encryption and signature schemes.

3 Volume I: Basic Tools

In this volume the author concentrates his attention on the basic tools of modern cryptography. The volume is divided into just four, rather large chapters, and two appendices.
Chapter 1 is an introduction, containing a high-level overview of the subject. Some background on probability and computational complexity is also presented here, as well as a motivation for needing a rigorous treatment.
The first, fundamental tool is presented in Chapter 2: one-way functions. These capture the very essence of cryptography: protecting confidential information from being retrieved by a malicious user. Hence, one-way functions are functions that are easy to compute, but hard to invert. They are described as a general tool, both at a basic level (strong and weak) and in a number of variants, such as universal one-way functions, trapdoor one-way permutations, hard-core predicates etc. The author also presents the most popular candidates for one-way functions, based on the hardness of a variety of mathematical problems; some examples are integer

factorization, decoding random linear codes, and the subset sum problem.
Chapter 3 is dedicated to another milestone of modern cryptography: pseudorandom generators. These primitives address one of the most important issues in the field, that is how to generate a random element, or sequence of elements. What pseudorandom generators do is generate a sequence that is computationally indistinguishable from a truly random one. The notion of computational indistinguishability is thus discussed, before defining pseudorandom generators and providing some examples of constructions. The remainder of the chapter features related concepts such as pseudorandom functions and pseudorandom permutations.
The conclusive chapter, Chapter 4, is entirely centered on zero-knowledge proofs systems. These protocols allow to prove that a certain assertion hold, without yielding anything beyond the validity of the assertion. They are particularly useful as a tool for building other cryptographic primitives. The author carefully lays out all the notions about zero-knowledge proof systems in its different aspects (interactive/non-interactive) and applications (witness indistinguishability, proofs of knowledge, identification schemes). Some negative results on the feasibility of zero-knowledge proofs and examples of constructions are also part of the chapter.
Finally, the appendices represent a helpful addition to the volume. In Appendix A, a few basic results on computational number theory are given. These include quadratic residues, primality tests, Legendre and Jacobi symbols, etc. In Appendix B, instead, there is a short summary of Volume II. Each section (Encryption, Signatures and Other protocols) is briefly introduced along some suggestions for further reading and for teaching.

4 Volume II: Basic Applications

The second volume complements and develops the material presented in the first, describing the main applications of the cryptographic tools just introduced. This is done, again, by grouping the content in few, but large chapters. There are three chapters, plus an additional appendix. The volume's numbering follows up from the previous, as to highlight the structure of the book as a whole.
Chapter 5 describes the first and fundamental of the cryptographic primitives: encryption schemes. For centuries cryptography was thought to be the art of constructing encryption schemes, and only recently (mid 1970's) developed into a family of applications, mainly thanks to the introduction of what is commonly known as "public-key" cryptography. The chapter gives a very rigorous treatment of both the private-key and public-key setting, introducing accurate security definitions and examples. All the most important security frameworks are defined, ranging from passive ("eavesdropping") attacks to very powerful ones such as chosen-plaintext and chosen-ciphertext attacks. Examples of encryption schemes include a simple version of "randomized" RSA, and the Blum-Goldwasser public-key scheme.
The second chapter, Chapter 6, is dedicated to another family of cryptographic primitives, with a purpose very different from that of encryption schemes: authentication. Thus, the chapter features both digital signature schemes and message authentication codes (MAC). Those were the first tasks to join encryption in forming modern cryptography, and they are now arguably as important. Once again, the presentation of these objects is very formal, and centered about security notions. Basic notions and constructions (e.g. one-time signatures) form the central part of the chapter. Several variants and alternative approaches to signature schemes are also described, such as incremental signatures and fail-stop signatures. The chapter is concluded, like the previous one, with miscellanous topics that include historical notes, suggestions for further reading, and open problems.
In the final chapter, Chapter 7, the focus is shifted onto the remaining cryptographic applications that were not treated before. These, called *General Cryptographic Protocols*, are mostly about general results on multi-party computation. The chapter begins by describing two-party computation, as a special case. Different attack models are presented, such as the semi-honest and the malicious model, and the concept of oblivious transfer is introduced. It then proceeds by presenting a protocol compiler, as a way of reducing between the two previously mentioned models, and finally generalizing the results to the multi-party setting. The case of perfect security in the private channel model is briefly treated in the last section, before the usual concluding miscellanea.
Lastly, Appendix C features a few additions and corrections to Volume I, such as enhanced trapdoor permutations and an additional discussion on non-interactive zero-knowledge proofs.

5 Style of the book

The book is very rigorous and systematic in its approach to the subject, as is the will of the author. The fact of having just few, large chapters makes them dense and rich of notions. Accurate definitions precede detailed and sometimes long proofs. Every chapter is also correlated with a few pages of exercises. In conclusion, the style is quite technical and austere.

6 Would you recommend the book?

The book provides a rigorous treatment of the theoretical foundations of cryptography. For the reasons discussed above, it can be sometimes hard to follow to an inexperienced reader, and it is best suited as a reference book for experts (as claimed by the author), or as a text book for a graduate course. I highly recommend the book to people in both these categories that are interested in a detailed approach to the subject.

The reviewer is a Post-doc at University of Warsaw, Poland.