Review of the book

"Complexity Theory and Cryptology — An Introduction to Cryptocomplexity"

by Jörg Rothe

Springer, 2005

ISBN: 3-540-22147-6, 978-3-540-22147-0

Rolf Oppliger
eSECURITY Technologies

March 9, 2010

1 What the book is about

This book is about complexity theory and its application in modern cryptology. The author has coined the term *cryptocomplexity* to refer to the symbiosis of the two research areas, i.e., *cryptology* and *complexity theory*. The term is well chosen and accurate; it adequately reflects the topic of the work. The resulting book is interesting and highly valuable for educational purposes, mainly because it yields a new and ingenious way to access modern cryptographic research results.

2 What is this book about (summary)?

As its title suggests, the book addresses cryptocomplexity and various aspects thereof. After a brief introduction in Chapter 1, it provides valuable background information about computer science and mathematics in Chapter 2. The information provided is well chosen and in line with the overall topic of the book. It includes algorithmics, formal languages and recursive function theory, logic, algebra, number theory, graph theory, and probability theory. In Chapter 3, the foundations of complexity theory are introduced and explained in detail. The notions of reducibility and completeness are particularly important in this context. Equipped with these notions, the foundations of cryptology are introduced in Chapter 4. The focus of this exposure is on classical encryption systems and perfect secrecy according to Shannon's Theorem and Vernam's one-time pad. In Chapter 5, some important complexity hierarchies built upon NP are introduced, such as the boolean hierarchy over NP and the polynomial hierarchy. In Chapter 6, randomized algorithms and complexity classes are explained in detail and put into perspective. Finally, the last two chapters address some aspects related to public key

cryptography. In Chapter 7, the RSA cryptosystem, primality testing, and the integer factorization problem are thoroughly discussed, whereas in Chapter 8, a few public key cryptosystems and protocols based on the discrete logarithm problem are introduced and put into perspective. Examples include Diffie-Hellman, Elgamal, and Rabin. Finally, the book comes along with complete lists of figures and tables, as well as a list of references and an index. In summary, the book provides a comprehensive and reasonably complete treatment of a topic that is located in-between cryptology and complexity theory.

3 What is the book like (style)?

The book is based on university lectures the author has hold in Germany since 1996. As such, it is a textbook in nature that is written in a scientific style. Theorems are introduced and rigorously proven in a mathematically sound way. The introductory part is a little bit dense, so anybody not familiar with the foundations of complexity theory and cryptology may want to look into complementary materials. This is particularly true for complexity theory, as the proper understanding of cryptocomplexity requires a profound familiarity in this matter. Alternatively speaking, somebody not well familiar with complexity theory may face a hard time in following and really understanding the main statements of the book. The book, in turn, does not provide a comprehensive handbook of all cryptographic algorithms and protocols in use today (there are many other books that can be used for this purpose). Instead, it introduces complexity-theoretic ideas and lines of argumentation, and applies them to cryptographic settings. The result is a new and ingenious way to access modern cryptographic research results. A reader of the book is likely to have a simpler access and require less time to understand the cryptographic proofs found in the literature. Experience shows that these proofs are particularly difficult to understand even for mathematicians who are not deeply involved in complexity theory and complexity-theoretic reasoning. Hence, this book has the potential to significantly simplify their research.

4 Would you recommend this book?

Yes, I would strongly recommend this book for anybody working on complexity theory or cryptology. Anybody working on complexity theory may profit from learning about applications in the realm of cryptology, whereas anybody working on cryptology may gain a lot from learning a mathematically precise way of introducing cryptographic primitives and proving their security. The target audience comprises undergraduate and graduate students in computer science, mathematics, and engineering, but the book is also recommended reading (and a valuable source of information) for researchers, university teachers, and practitioners working in the field. Furthermore, it is exceptionally well suited for self-study. This makes the book so unique that it should be part of any library on cryptology or complexity theory.

The reviewer is an adjunct professor at the University of Zurich (Switzerland).