Review of the book

"Digital Signatures"
by Jonathan Katz
Springer, 2010

ISBN: 978-0-387-27711-0

Vincenzo Iovino
University of Luxembourg

1 What is the book about?

This book covers a complete and self-contained monograph on digital signatures, one of the major protocols in cryptography.

Digital signatures are a digital analogue of traditional signatures used in everyday life and can be used for signing documents over the internet or for more complex protocols. This treatise presents the descriptions of the most famous signature schemes as well as the theoretical principles and foundations used in their design.

The book is intended for students, both at an undergraduate or graduate level, or practitioners with a previous background in the basics of modern cryptography (whose coverage can be found in the textbook *Modern Cryptography* co-authored by the same author). Likewise, it can benefit researchers in the field looking for an extended treatment of "folklore" results that are spread out over a vast literature.

The style of the author is rigorous with formal definitions and proofs and it will be better appreciated by readers familiar with the principles and tools of *provable security.* Any topic is discussed in length and depth and motivated by concrete examples.

This text is the only book exclusively dedicated to digital signatures but notwithstanding covers related topics like hash functions and identification schemes.

2 Summary of the book

2.1 Part I: Setting the Stage

This part starts with an overview of digital signatures and its applications and then introduces the necessary background at an accessible level. All major definitions used in literature are presented, including more advanced ones that could skipped at a first reading and recalled only when necessary.

Chapter 1 contains a deep presentation of the relations between these notions, and classical results like constructions of strong unforgeable signature schemes from unforgeabile ones, and improvements for extending the message length and reducing the public-key length. Furthermore, in Chapter 2 the authors recalls the standard hardness assumptions used to construct digital signature.

As in the style of the author, any definition is motivated by a concrete real-world example before being studied within a theoretical framework.

2.2 Part II: Digital Signature Schemes without Random Oracles

This part covers the constructions of digital signatures both from general assumptions and from specific number specific assumptions. Chapter 3 explores in detail constructions based on minimal assumptions and as such efficiency is of no importance here. In fact, these general constructions have as drawbacks computational inefficiency and very long signatures but offer the advantage of being *general* and *simple* to explain. Moreover they remain a fundamental tool due to the possibility of instantiating them from general primitives like one-way functions with different classes of specific functions.

The author describes the seminal Lamport's construction of one-time signature schemes. He then proceeds to present the tree-based construction of full-fledged signatures from any one-time scheme with message space twice as long as the verification key. Finally, he concludes by putting the pieces together to get a (full) signature scheme from any one-way function.

The remaining two chapters of this section feature constructions based on the RSA assumption and on bilinear maps, two fundamental tools largely used in cryptography.

As is usual throughout the book, this part is followed by a nice historical overview on the development of signature schemes and on the *race* to the minimal assumptions which they can be based on.

2.3 Part III: Digital Signature Schemes in the Random Oracle Model

The random oracle model is a theoretical framework and methodology to design practical cryptographic primitives. Though this model is very debated and raises theoretical drawbacks, it has been proven successful in the design of very *efficient* signature schemes. The random oracle model is one of the concepts of modern cryptography least easy to understand for newcomers but the authors does a great work in making this accessible to the non-experts in the area. The author describes the topic with concrete examples from the literature and motivates it step by step providing intuitions and technicalities easy to digest.

Chapter 6 is thus devoted to theoretical considerations about the random oracle methodology. In Chapter 7 the author presents the construction of full-domain hash signature schemes in the random oracle model and its variants. Chapter 8 provides various constructions of signature schemes from identification schemes and related techniques, like the Fiat-Shamir scheme and transform, and the schemes of Guillou-Quisquater, Micali-Ong, and Schnorr.

3 Would you recommend this book?

The book contains the broadest coverage of signature schemes and as such is unique among the books on cryptography. The author is one of the biggest experts of cryptography, author of other books and of hundreds of scientific papers in the field.

The book may be of extreme importance both for a beginner and for a researcher. The former can benefit from the comprehensive account of the definitions and theoretical tools designed for signature schemes (but that can be also applicable to other cryptographic primitives and protocols), and from the very nice historical sections added at the end of any chapter that can help to reconstruct the relevant literature in the field.

The latter can use it as a self-contained reference for a so vast area of research spread over a large amount of papers emerged in the last 30 years, and for valuable discussions of some aspects that are often skipped in the literature.

The text will be also of use to practitioners and programmers interested in the details of signature schemes.

This book is a masterpiece and cannot be missing in the bookshelf of a real cryptographer.

The only "drawback" of the book, if there has to be one, is that bilinear maps are only *assumed* to exist without providing details on their implementation. I think that this is justifiable due to the difficulties to present the relevant background necessary to fully understand and construct bilinear maps. In fact, the mathematics of elliptic curves and bilinear maps are beyond the scope of the book and can be found in other books. Nevertheless, this gap does not affect the understandability of the constructions of signature schemes based on bilinear maps, since bilinear maps can be used as black-box without knowledge of their implementation details.

The reviewer is a post-doc at the University of Luxembourg.