Digital Signatures

Jonathan Katz

Digital Signatures

Jonathan Katz
Department of Computer Science
University of Maryland
A.V. Williams Bldg.
College Park, MD 20742
USA
jkatz@cs.umd.edu

ISBN 978-0-387-27711-0 e-ISBN 978-0-387-27712-7
DOI 10.1007/978-0-387-27712-7
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010927931

To Jill, Abigail, and Rena

Preface

As a beginning graduate student, I recall being frustrated by a general lack of accessible sources from which I could learn about (theoretical) cryptography. I remember wondering: *why aren't there more books presenting the basics of cryptography at an introductory level?* Jumping ahead almost a decade later, as a faculty member my graduate students now ask me: *what is the best resource for learning about (various topics in) cryptography?* This monograph is intended to serve as an answer to these questions — at least with regard to digital signature schemes.[1]

Given the above motivation, this book has been written with a beginning graduate student in mind: a student who is potentially interested in doing research in the field of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next. Though intended primarily for that audience, I hope that advanced graduate students and researchers will find the book useful as well. In addition to covering various constructions of digital signature schemes in a unified framework, this text also serves as a compendium of various "folklore" results that are, perhaps, not as well known as they should be. This book could also serve as a textbook for a graduate seminar on advanced cryptography; in such a class, I expect the entire book could be covered at a leisurely pace in one semester with perhaps some time left over for excursions into related topics. I hope it will also prove helpful to graduate students and researchers in other fields, such as computer security or mathematics, who want to obtain a more thorough appreciation of digital signatures and known results in this area.

The only real prerequisite for this book is a previous course (at the undergraduate or graduate level) covering the basic foundations of modern cryptography. Specifically, I assume the reader has taken a course whose coverage and treatment of cryptography is similar to that of the textbook *Introduction to Modern Cryptography* [72] that I have co-authored with Yehuda Lindell. Comfortability with formal definitions and proofs is expected, and it is assumed the reader is already familiar with, e.g., the RSA and discrete logarithm problems, and the notion of one-way

[1] Fortunately, the past few years have seen the publication of some excellent books providing an introduction to the field as a whole, as well as books covering other specific topics in cryptography.

functions. While I have made an effort to introduce all the necessary background material as needed, the reader will find things much more easy going if they have encountered this background material previously.

The current book is divided into three sections:

- *Part I — Setting the Stage.* This part includes relevant background material, an overview of digital signatures, and definitions of security for signature schemes. Even readers with a firm background in cryptography should skim this part of the book since the definitions given here include "non-standard" ones such as security against known-/random-message attacks, and "strong" security for signature schemes.
- *Part II — Digital Signature Schemes without Random Oracles.* Parts II and III of the book cover constructions of digital signature schemes. Part II focuses on schemes that can be proven secure without resorting to the "random oracle" model. (A brief introduction to the random oracle model is provided in Chapter 6.) This part begins with the important theoretical result showing that signatures can be constructed from any one-way function (though a complete proof is given only for the case of one-way permutations). Next, constructions based on the RSA and strong RSA assumptions are presented. Finally, some more recent constructions of signature schemes from bilinear maps are shown.

  To my knowledge, Part II describes essentially all known classes of signature schemes that do not rely on the random oracle model.
- *Part III — Digital Signature Schemes in the Random Oracle Model.* The signature schemes considered in Part II are, generally speaking, considered too inefficient for practical use. Instead, more efficient schemes with proofs of security in the random oracle model are used. Following a brief introduction to the random oracle model (along with a discussion of its pros and cons), we discuss the two main approaches used in constructing signatures in this setting: building signatures from identification schemes, and designing signatures using trapdoor permutations (or variants thereof) and the "hash-and-sign" approach.

Unfortunately omitted in this work is any discussion of signature schemes based on specific, "non number-theoretic" assumptions including those based on knapsacks, lattices, coding theory, or polynomial equations. I have also decided to focus only on "standard" signature schemes and not to cover any of the multitude of variants (e.g., undeniable, ring, group, homomorphic, ... signature schemes) that are out there. From a basic theoretical perspective, however, this book is fairly comprehensive and will, I hope, serve as a useful primer for the more specialized literature.

Comments and Errata

I am always happy to receive feedback and constructive criticism enabling me to improve this book. I am also always grateful (though less happy) to hear about any

errors or omissions. Please email any comments to jkatz@cs.umd.edu with "Digital Signatures Book" in the subject line.

Acknowledgments

It gives me great pleasure to acknowledge the unwavering support of my wife, Jill, during the time I wrote this book. I would also like to thank Yehuda Lindell and Bob Stern for allowing me to adapt some of the text from [72] for inclusion here. Finally, I would like to thank Susan Lagerstrom-Fife for her patience and encouragement (prodding?) during the course of this project.

Portions of this book were written during my sabbatical year at IBM. I am grateful to Tal Rabin and all the members of the crypto research group at IBM for being such wonderful hosts.

My work on this book was supported in part by the National Science Foundation under grants #0447075, #0627306, and #0716651. Any opinions, findings, conclusions, or recommendations expressed in this book are my own, and do not necessarily reflect the views of the National Science Foundation.

College Park, MD *Jonathan Katz*
March 2010

Contents

Part III Digital Signature Schemes in the Random Oracle Model