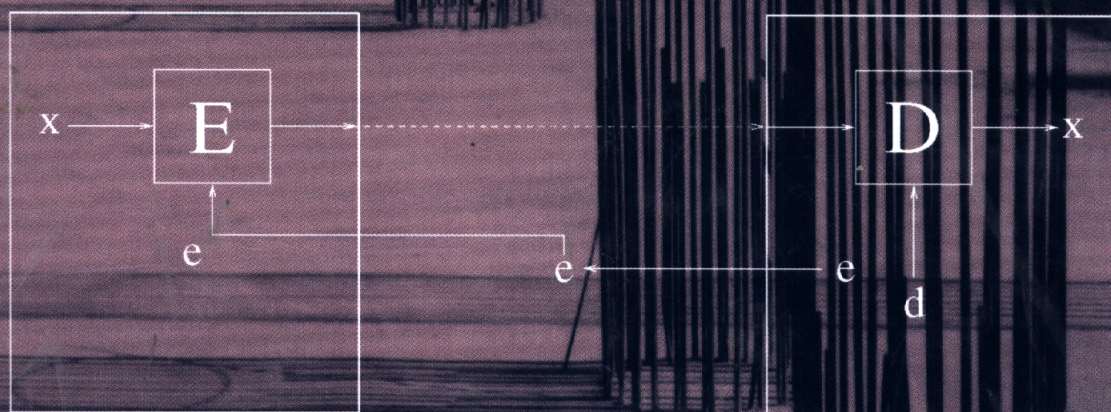


FOUNDATIONS OF CRYPTOGRAPHY

Volume II Basic Applications



ODED GOLDREICH

Foundations of Cryptography

Cryptography is concerned with the conceptualization, definition, and construction of computing systems that address security concerns. The design of cryptographic systems must be based on firm foundations. *Foundations of Cryptography* presents a rigorous and systematic treatment of foundational issues: defining cryptographic tasks and solving new cryptographic problems using existing tools. The emphasis is on the clarification of fundamental concepts and on demonstrating the feasibility of solving several central cryptographic problems, as opposed to describing ad hoc approaches.

This second volume contains a rigorous treatment of three basic applications: encryption, signatures, and general cryptographic protocols. It builds on the previous volume, which provides a treatment of one-way functions, pseudorandomness, and zero-knowledge proofs. It is suitable for use in a graduate course on cryptography and as a reference book for experts. The author assumes basic familiarity with the design and analysis of algorithms; some knowledge of complexity theory and probability is also useful.

Oded Goldreich is Professor of Computer Science at the Weizmann Institute of Science and incumbent of the Meyer W. Weisgal Professorial Chair. An active researcher, he has written numerous papers on cryptography and is widely considered to be one of the world experts in the area. He is an editor of *Journal of Cryptology* and *SIAM Journal on Computing* and the author of *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*.

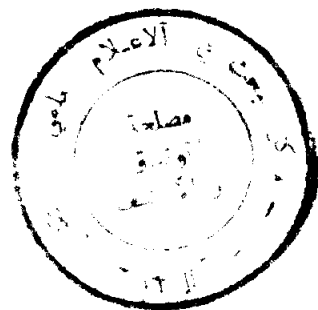
BIBLIOTHEQUE DU CERIST

Foundations of Cryptography

II Basic Applications

Oded Goldreich

Weizmann Institute of Science



BIBLIOTHEQUE DU CERIST



PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

<http://www.cambridge.org>

© Oded Goldreich 2004

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2004

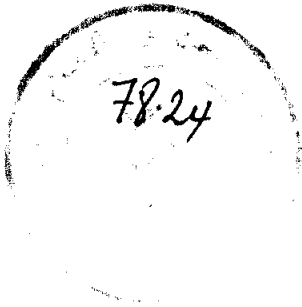
Printed in the United States of America

Typefaces Times New Roman 10.5/13 pt. and Helvetica Neue Regular *System* L^AT_EX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication data available

ISBN 0 521 83084 2 hardback
ISBN 0 521 79172 3 Volume I



BIBLIOTHEQUE DU CERIST

To Dana

BIBLIOTHEQUE DU CERIST

Contents

II Basic Applications



List of Figures	<i>page xi</i>
Preface	xiii
Acknowledgments	xxi
5 Encryption Schemes	373
5.1. The Basic Setting	374
5.1.1. Private-Key Versus Public-Key Schemes	375
5.1.2. The Syntax of Encryption Schemes	376
5.2. Definitions of Security	378
5.2.1. Semantic Security	379
5.2.2. Indistinguishability of Encryptions	382
5.2.3. Equivalence of the Security Definitions	383
5.2.4. Multiple Messages	389
5.2.5.* A Uniform-Complexity Treatment	394
5.3. Constructions of Secure Encryption Schemes	403
5.3.1.* Stream-Ciphers	404
5.3.2. Preliminaries: Block-Ciphers	408
5.3.3. Private-Key Encryption Schemes	410
5.3.4. Public-Key Encryption Schemes	413
5.4.* Beyond Eavesdropping Security	422
5.4.1. Overview	422
5.4.2. Key-Dependent Passive Attacks	425
5.4.3. Chosen Plaintext Attack	431
5.4.4. Chosen Ciphertext Attack	438
5.4.5. Non-Malleable Encryption Schemes	470
5.5. Miscellaneous	474
5.5.1. On Using Encryption Schemes	474
5.5.2. On Information-Theoretic Security	476
5.5.3. On Some Popular Schemes	477

CONTENTS

5.5.4.	Historical Notes	478
5.5.5.	Suggestions for Further Reading	480
5.5.6.	Open Problems	481
5.5.7.	Exercises	481
6	Digital Signatures and Message Authentication	497
6.1.	The Setting and Definitional Issues	498
6.1.1.	The Two Types of Schemes: A Brief Overview	498
6.1.2.	Introduction to the Unified Treatment	499
6.1.3.	Basic Mechanism	501
6.1.4.	Attacks and Security	502
6.1.5.*	Variants	505
6.2.	Length-Restricted Signature Scheme	507
6.2.1.	Definition	507
6.2.2.	The Power of Length-Restricted Signature Schemes	508
6.2.3.*	Constructing Collision-Free Hashing Functions	516
6.3.	Constructions of Message-Authentication Schemes	523
6.3.1.	Applying a Pseudorandom Function to the Document	523
6.3.2.*	More on Hash-and-Hide and State-Based MACs	531
6.4.	Constructions of Signature Schemes	537
6.4.1.	One-Time Signature Schemes	538
6.4.2.	From One-Time Signature Schemes to General Ones	543
6.4.3.*	Universal One-Way Hash Functions and Using Them	560
6.5.*	Some Additional Properties	575
6.5.1.	Unique Signatures	575
6.5.2.	Super-Secure Signature Schemes	576
6.5.3.	Off-Line/On-Line Signing	580
6.5.4.	Incremental Signatures	581
6.5.5.	Fail-Stop Signatures	583
6.6.	Miscellaneous	584
6.6.1.	On Using Signature Schemes	584
6.6.2.	On Information-Theoretic Security	585
6.6.3.	On Some Popular Schemes	586
6.6.4.	Historical Notes	587
6.6.5.	Suggestions for Further Reading	589
6.6.6.	Open Problems	590
6.6.7.	Exercises	590
7	General Cryptographic Protocols	599
7.1.	Overview	600
7.1.1.	The Definitional Approach and Some Models	601
7.1.2.	Some Known Results	607
7.1.3.	Construction Paradigms	609

CONTENTS

7.2.* The Two-Party Case: Definitions	615
7.2.1. The Syntactic Framework	615
7.2.2. The Semi-Honest Model	619
7.2.3. The Malicious Model	626
7.3.* Privately Computing (Two-Party) Functionalities	634
7.3.1. Privacy Reductions and a Composition Theorem	636
7.3.2. The OT_1^k Protocol: Definition and Construction	640
7.3.3. Privately Computing $c_1 + c_2 = (a_1 + a_2) \cdot (b_1 + b_2)$	643
7.3.4. The Circuit Evaluation Protocol	645
7.4.* Forcing (Two-Party) Semi-Honest Behavior	650
7.4.1. The Protocol Compiler: Motivation and Overview	650
7.4.2. Security Reductions and a Composition Theorem	652
7.4.3. The Compiler: Functionalities in Use	657
7.4.4. The Compiler Itself	681
7.5.* Extension to the Multi-Party Case	693
7.5.1. Definitions	694
7.5.2. Security in the Semi-Honest Model	701
7.5.3. The Malicious Models: Overview and Preliminaries	708
7.5.4. The First Compiler: Forcing Semi-Honest Behavior	714
7.5.5. The Second Compiler: Effectively Preventing Abort	729
7.6.* Perfect Security in the Private Channel Model	741
7.6.1. Definitions	742
7.6.2. Security in the Semi-Honest Model	743
7.6.3. Security in the Malicious Model	746
7.7. Miscellaneous	747
7.7.1.* Three Deferred Issues	747
7.7.2.* Concurrent Executions	752
7.7.3. Concluding Remarks	755
7.7.4. Historical Notes	756
7.7.5. Suggestions for Further Reading	757
7.7.6. Open Problems	758
7.7.7. Exercises	759
Appendix C: Corrections and Additions to Volume 1	765
C.1. Enhanced Trapdoor Permutations	765
C.2. On Variants of Pseudorandom Functions	768
C.3. On Strong Witness Indistinguishability	768
C.3.1. On Parallel Composition	769
C.3.2. On Theorem 4.6.8 and an Afterthought	770
C.3.3. Consequences	771
C.4. On Non-Interactive Zero-Knowledge	772
C.4.1. On NIZKs with Efficient Prover Strategies	772
C.4.2. On Unbounded NIZKs	773
C.4.3. On Adaptive NIZKs	774

CONTENTS

C.5.	Some Developments Regarding Zero-Knowledge	775
C.5.1.	Composing Zero-Knowledge Protocols	775
C.5.2.	Using the Adversary's Program in the Proof of Security	780
C.6.	Additional Corrections and Comments	783
C.7.	Additional Mottoes	784
Bibliography		785
Index		795

Note: Asterisks indicate advanced material.