ADVANCES IN INFORMATION SECURITY

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY

BIBLIOTHEQUE DU CERIST

Song Y. Yan

Kluwer Academic Publishers

IST 2902

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY

BIBLIOTHEQUE DU CERIST

Advances in Information Security

Sushil Jajodia
Consulting editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

BIBLIOTHEQUE DU CERIST

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers as well as developers are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
APPLICATIONS OF DATA MINING IN COMPUTER SECURITY, edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3
MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1
TRUSTED RECOVERY AND DEFENSIVE INFORMATION WARFARE by Peng Liu and Sushil Jajodia, ISBN: 0-7923-7572-6
RECENT ADVANCES IN RSA CRYPTOGRAPHY by Stefan Katzenbeisser, ISBN: 0-7923-7438-X
E-COMMERCE SECURITY AND PRIVACY by Anup K. Ghosh, ISBN: 0-7923-7399-5
INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia, ISBN: 0-7923-7204-2

Additional information about this series can be obtained from
http://www.wkap.nl/prod/s/ADIS

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY

by

Song Y. Yan
Coventry University, United Kingdom

KLUWER ACADEMIC PUBLISHERS
Boston / Dordrecht / London

BIBLIOTHEQUE DU CERIST

Distributors for North, Central and South America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061 USA
Telephone (781) 871-6600
Fax (781) 871-6528
E-Mail <kluwer@wkap.com>

Distributors for all other countries:
Kluwer Academic Publishers Group
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS
Telephone 31 78 6576 000
Fax 31 78 6576 474
E-Mail <orderdept@wkap.nl>

Electronic Services <http://www.wkap.nl>

Library of Congress Cataloging-in-Publication

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY
by Song Y. Yan
ISBN: 1-4020-7649-5

7821

Copyright © 2004 by Kluwer Academic Publishers

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photo-copying, microfilming, recording, or otherwise, without the prior written permission of the publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.
Permissions for books published in the USA: permissions@wkap.com
Permissions for books published in Europe: permissions@wkap.nl

Printed on acid-free paper.

Printed in the United States of America

BIBLIOTHEQUE DU CERIST

Dedicated to Professor Shiing-Shen Chern

for his 92nd Birthday

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Preface

The problem of distinguishing prime numbers from composite, and of resolving composite numbers into their prime factors, is one of the most important and useful in all arithmetic. ... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated.

C. F. GAUSS (1777–1855)

Primality testing and integer factorization, as identified by Gauss in his *Disquisitiones Arithmeticae*, Article 329, in 1801, are the two most fundamental problems, as well as two most important research fields in number theory, particularly in *computational* number theory[1]. With the advent of digital computers, they have also been found unexpected and surprising applications in computing and particularly in cryptography and information security. In this book, we shall introduce various methods/algorithms for primality testing and integer factorization, and their applications in public-key cryptography and information security. More specifically, we shall first review some basic concepts and results in number theory in Chapter 1. Then in Chapter 2 we shall discuss various algorithms for primality testing and prime number generation, with an emphasis on the Miller-Rabin probabilistic test, the Goldwasser-Kilian and Atkin-Morain elliptic curve tests, and the Agrawal-Kayal-Saxena deterministic test. There is also an introduction to large prime number generation in Chapter 2. In Chapter 3 we shall introduce various algorithms, particularly the Elliptic Curve Method (ECM), the Quadratic Sieve (QS) and the Number Field Sieve (NFS) for integer factorization. Also in Chapter 3 we shall discuss some other computational problems that are related to factoring, such as the square root problem, the discrete logarithm problem and the quadratic residuosity problem. In Chapter 4, we shall discuss

[1] Of course, the primality testing problem (PTP) has *now* been solved, thanks to Agrawal, Kayal and Saxena [5]. That is, the PTP can now be solved in $\mathcal{P}$ (deterministic polynomial-time). However, the integer factorization problem (IFP) is still open. That is, we still do not have an efficient (i.e., deterministic polynomial-time) algorithm for IFP; in the author's opinion, the IFP may indeed be an $\mathcal{NP}$-hard problem, although no proof can be given yet at present.

BIBLIOTHEQUE DU CERIST

some of the most widely used cryptographic systems based on the computationally intractable problems such as integer factorization, square roots, quadratic residuosity, discrete logarithms, and elliptic curve discrete logarithms.

We have tried to make this book as self-contained as possible, so that it can be used either as a textbook suitable for a course for final-year undergraduate or first-year postgraduate students, or as a basic reference in the field.

Acknowledgments

I would like to thank the three anonymous referees for their very helpful comments and kind encouragements. I would also like to thank Susan Lagerstrom-Fife and Sharon Palleschi of Kluwer Academic Publishers in Boston, and Prof. Sushil Jajodia of George Mason University, Editor of the Advances in Information Security Series, for their encouragement and help. Special thanks must be given to Dr. Bob Newman for his genius support during the preparation of this book, and to Dr. Nick Godwin for proofreading the final manuscript of the book. Finally, I would like to thank Prof. Martin Hellman, Stanford University and Prof. Shiing-Shen Chern, Director Emeritus of the Mathematical Sciences Research Institute in Berkeley for their kind encouragement and guidance.

Coventry, September 2003 S. Y. Y.

BIBLIOTHEQUE DU CERIST

Table of Contents

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST