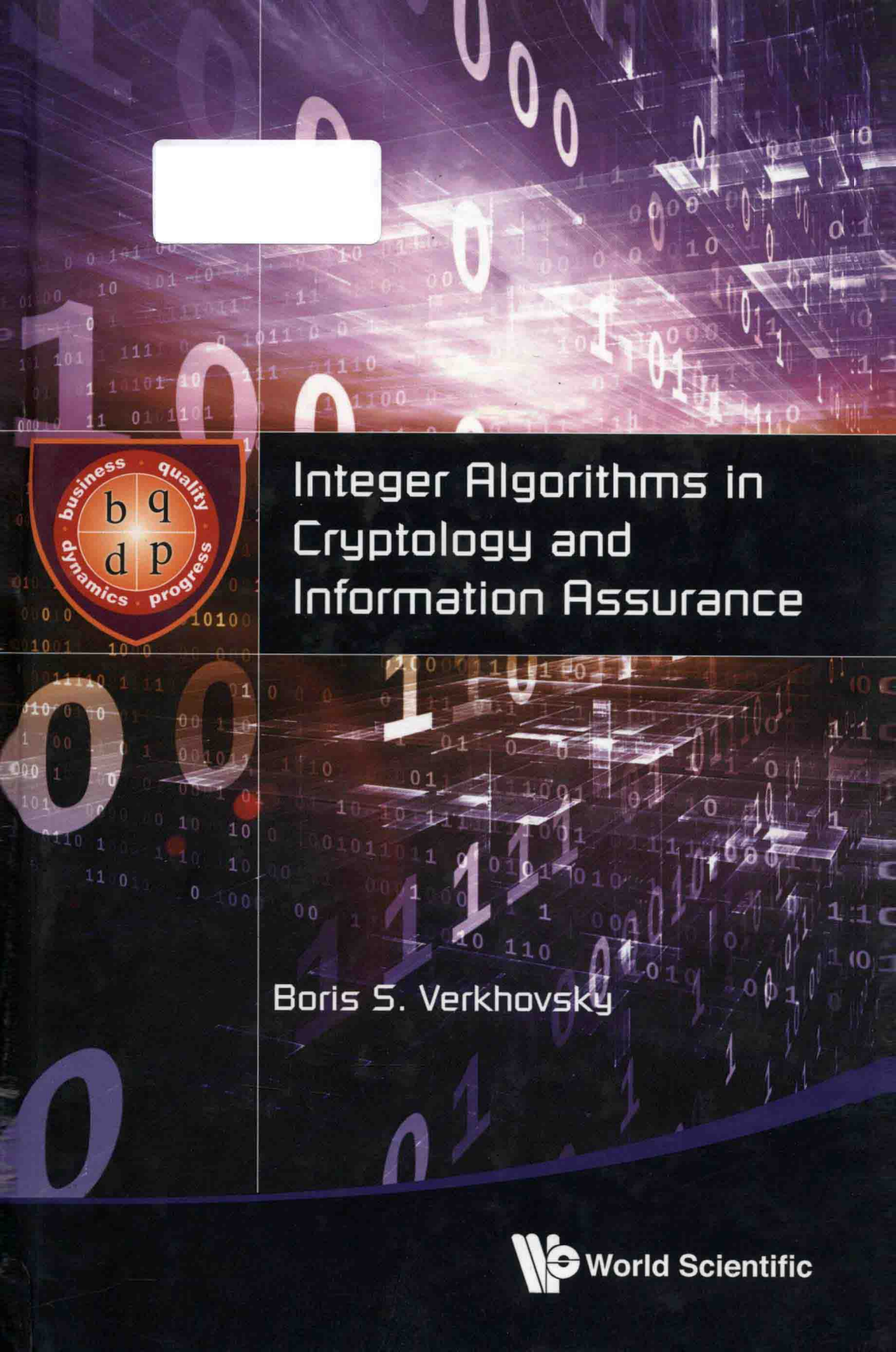
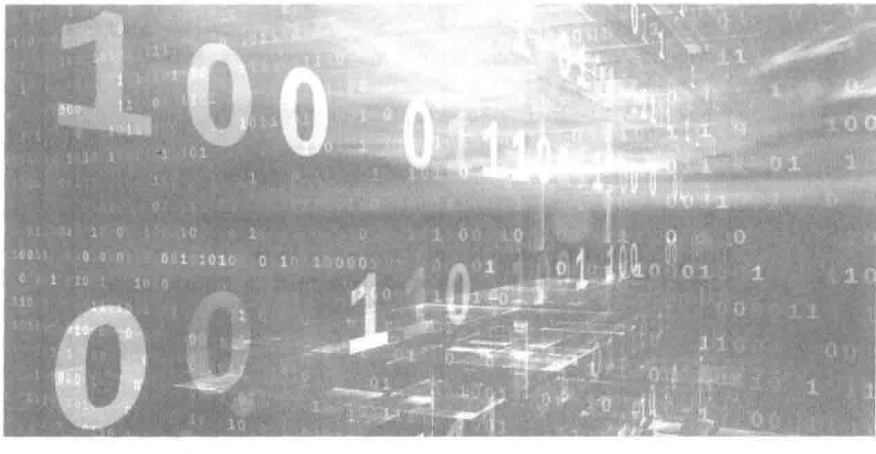


Integer Algorithms in Cryptology and Information Assurance

Boris S. Verkhovsky

World Scientific

Integer Algorithms in Cryptology and Information Assurance



Boris S. Verkhovsky
New Jersey Institute of Technology, USA

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Cataloging-in-Publication Data

Verkhovsky, Boris S.

Integer algorithms in cryptology and information assurance / prof. Boris S. Verkhovsky, New Jersey Institute of Technology, USA.

pages cm

Includes bibliographical references

ISBN 978-9814623742 (hardback : alk. paper)

1. Information technology--Mathematics. 2. Cryptography--Mathematics. 3. Data integrity. 4. Algorithms. 5. Numbers, Natural. 6. Number theory. I. Title.

T58.5.V47 2014

652'.8015181--dc23

2014024555

British Library Cataloguing-in-Publication Data

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

In-house Editor: Amanda Yun

Typeset by Stallion Press

Email: enquiries@stallionpress.com

Printed in Singapore

Integer Algorithms in Cryptology and Information Assurance

About the Author

Dr. Boris S. Verkhovsky is a Professor of Computer Science at the New Jersey Institute of Technology (NJIT). He received his PhD in Computer Science jointly from the Academy of Sciences of the USSR and the Latvia State University, Riga.

Professor Verkhovsky's research experience and interests span across communication security, design and analysis of cryptosystems and information assurance protocols, the design and control large-scale systems, optimization and algorithms, and the design and control of telecommunication networks.

His prior affiliations are: the Scientific Research Institute of Computers (Moscow), the Academy of Sciences of the USSR, Princeton University School of Engineering, IBM Thomas J. Watson Research Center (Yorktown Heights), Bell Laboratories, University of Colorado and, since 1986, the NJIT.

Professor Verkhovsky is a recipient of awards including the USSR Ministry of Radio-Electronics Award; the Academy of Sciences of the USSR Award; the Alvin Johnson Award; and the Millennium Award and Medal of Excellence. Professor Verkhovsky is also a recipient of Blasé Pascal Award and Medal, and is listed in Marquis *Who's Who in America.*

Verkhovsky was the Wallace J. Eckert Scientist at the IBM Thomas J. Watson Research Center, a Member of Technical Staff at Bell Labs, and held the Charles Dana Endowed Chair Professorship. In 2002 he was elected as a member, and in 2003, as a Fellow of the European Academy of Science (EAS). He served as the EAS's Vice President from 2003 till 2006.

Dedicated to my children
Ekaterina-Anastasia and Samuel,
And in memoriam of my parents
Samuel and Alla Verkhovsky

Preface

"If you are out to describe the truth,
Leave elegance to the tailor",

A. Einstein

This book is based on the author's research and computer experiments for the last several years. It is mostly devoted to the discussion of algorithmic aspects that were developed and analyzed by the author for secure and reliable transmission of information and digital authentication of senders over open communication channels. The book consists of several parts describing and analyzing basic algorithms in modular arithmetic; cryptographic protocols based on complex moduli; algorithms for information assurance; cryptanalytic algorithms solving discrete logarithm problem (DLP); methods of cryptanalysis for solution of integer factorization (iFac) based on a generalization of Gauss's theorem; hybrid algorithms for information assurance and cryptography; cryptographic algorithms based on three-dimensional elliptic surfaces; sender identification/digital signature algorithms; and search and design algorithms that are provided in the last several chapters.

The algorithms considered in this book are designed for integer arithmetic of multi-digit long numbers. The reason to consider integer arithmetic stems from the necessity to deal with extremely large integers, which are used for secure encryption of sensitive information transmitted via communication channels that are open both to designated receivers as well as to unauthorized intruders. Various arithmetic transformations based on additions, subtractions, multiplications and exponentiations of integers are used for the encryption. Although each of these operations preserve the integer character of numerically-presented information, the size of the resulting integers is far beyond what computers can handle unless

we use scientific notations and round off the extremely large numbers consisting of tens of thousands or more digits. However, rounding off is absolutely unacceptable in our case, otherwise after numerous operations the rounding off errors will propagate and, as a result, we will not be able to recover on the decryption level the initially transmitted information and instead of encrypted and transmitted "*Princeton*" the receiver will decrypt "*Pinkerton*" or instead of encrypted and transmitted "*Evian Bonus*" the receiver will decrypt "*Naïve Lotus*". Another obstacle in dealing with integers is that on the level of decryption we need to use *inverse* arithmetic operations (division, extraction of roots etc.). However, in the overwhelming majority of cases these inverse operations do not preserve integrality of inputs since in traditional arithmetic *seven divided by three* is not an integer, and in the relatively small interval $[1, 10^6]$ only one thousands integers have exact integer square roots, only one hundred of them have exact integer cubic roots etc. The magic of modular arithmetic resolves most of these "problems" very efficiently. Indeed, seven-divided-by-three only in exceptional cases does not have an integer output (and we are aware of these limitations). For the interval mentioned above exactly half a million integers (versus 1,000 in traditional arithmetic) have integer square roots (and, of course, we know under what conditions that happens). Certainly, to make everything work efficiently we need to address many other issues to be sure that all processes are executed fast enough, with assured correctness and without undesirable surprises.

Here it is important to mention that there is a substantially distinct methodology in dealing with problems in mathematics of real numbers and modular arithmetic of integers. In the former case many classes of problems are solvable via efficient algorithms because the class of objects in many problems has global characteristics like continuity, convexity or concavity, unimodality or bi-modality, separability, existence of contracting operators, etc. However, in the modular arithmetic in most of cases the class of objects under study does not have global properties with one important exception. In the middle of the seventeenth century Pierre Fermat noticed that if modulus p is a prime, then for every integer c not divisible by p holds a cyclic property that $c^p \bmod p = c$. This is known as Fermat Little Theorem that was generalized by the Swiss mathematician Leonhard Euler: if $n = pq$, where p and q are primes, then for every c relatively prime with n the cyclic property holds: $c^{n-p-q+2} \bmod n = c$.

This property is in the core of RSA public-key cryptography. As it is shown in several chapters of this book, there are analogous cyclic

properties in modular arithmetic based on complex integers and on complex moduli.

In dealing with efficiency and correctness of computation and other goals an inventive approach is a must. Such an approach is presented in this book for readers, who are interested in the proposed algorithms. The stress in the presentation of these algorithms is mostly on the descriptive and constructive levels rather than on the validation of algorithms (the mathematical proofs). Only in exceptional cases are the proofs presented. That is why many statements in the books are provided as conjectures or like propositions without proofs.

The proposed algorithms have numerous applications in business, banking, engineering, telemedicine (in laparoscopic surgery and implantable medical devices), in monitoring of containers in foreign trade exchange, in the national system of cybersecurity, in military systems, in interplanetary Internet developed by NASA for space research (monitoring and control of space vehicles, rovers/robots, and telemedicinal monitoring of astronauts), and many other areas of communication and control.

In the first several chapters of the book we describe various algorithms in modular arithmetic (modular multiplicative inverse algorithm, deterministic selection of generators, multiplication of multi-digit large integers, primality-testing procedures, etc.). These algorithms play significant roles in modern cryptographic protocols. Many combinatorial problems can be solved via a sequential analysis of permutations in conjunction with the branch-and-bound approach. The traveling salesman problem is an example of such a problem. Random permutations are used for inter-processor communication (randomized routing algorithm), in parallel computers and in various cryptographic schemes: substitution, transposition or permutation. Chapter 5 describes algorithms that both generate the permutations and count them.

In the second part of the book we provide various encryption/decryption algorithms based on complex moduli rather than on real moduli. As we show in the book, the modular arithmetic based on the complex integer modulus (p, q) creates cycles of order $p^2 + q^2$ while the arithmetic with real modulus p has cycles of order p. Therefore, for potential intruders/cryptanalysts the computational complexity to solve inverse problems like the iFac of semi-primes or the DLP is significantly higher in the complex-moduli arithmetic than in the arithmetic based on real moduli. For instance, if both p and q are one hundred decimal-digits long integers, then the modulus (p, q) creates a cycle of 200-digit long,

while in real-modulus arithmetic the cycle is the same as modulus p, i.e., 100 digits large. Hence, if the size of the cycle is a measure of cryptographic protection (crypto-immunity), then in the complex modular arithmetic we have 100-digit large cycle if either p or q or both are 50-digit long integers. As a result, we need to perform all computations with integers that are 10^{50} times smaller than their counterparts in the arithmetic based on the real moduli. Therefore, the time complexity of encryption and decryption can be substantially reduced, i.e., the cryptographic protocols can be executed faster, which is important if we wish to eventually implement them in a real-time mode.

A hybrid cryptographic system described in Chapter 13 provides also digital signature of the sender (sender identification) that transmits the information.

In modern communication networks two major requirements must be satisfied: the reliability of connection and the security of delivery. The implementation of these two requirements of information processing consumes extra time and additional bandwidth. These are major drawbacks if rapid delivery is essential. Information transmissions in a military environment and in financial exchanges are examples in which delay is a sensitive issue.

In the third part we describe several algorithms for reliable and secure transmission of information via open communication channels with random errors. These algorithms are based on various protocols of the information assurance and recovery of initially-transmitted data. Several reliability protocols are described in this part. Their characteristics (probabilities of protocol failure, specific bandwidth requirement per block of transmitted information and complexity of recovery) are analyzed and compared.

In addition to reliability and security, real-time communication in a voice network over the Internet is the time constraint that is even tighter since a delay larger than a quarter of a second is not acceptable. The efficiency of these protocols from various points of view, including the probability of failure and bandwidth requirement, we discuss in that part of the book. We also demonstrate that in some specially-tailored protocols, proposed by the author of this book, the information recovery is a straightforward process, while in other cases it is extremely tedious.

In the book we describe and analyze algorithms that assure a high probability of information transmission over unreliable channels and simultaneously provide protection of information from uninitiated and sometimes malicious intruders. It is shown that hybrid algorithms dealing

simultaneously with information assurance and security are synergistically more efficient from a computational point of view in comparison with separate application of security and information assurance protocols. Tables, figures and numerous examples illustrate various concepts described in this part of the book.

In the fourth part, we dedicated to the system design and cryptanalytic algorithms dealing primarily with computational complexity of iFac and DLP. On the system design level of cryptographic protocols it is essential to select their basic parameters that satisfy certain conditions. For instance, in the classical Diffie–Hellman key exchange (DHKE) protocol, as well as in the RSA, Rabin, ElGamal and other cryptographic protocols it is required that the corresponding keys of the communicating parties must be prime integers. In the algorithms that we discuss in the second part it is essential to select, on the system design level, complex integers that are primes. Although it is not computationally difficult to verify whether given (p, q) is a complex prime, it is much more challenging to directly select a large (p, q) that *is* a complex prime. Chapter 22 provides an indirect and computationally efficient algorithm that solves this problem. That algorithm is based on the author's generalizations of Gauss's Theorem (GGT) and on the existing algorithms that count how many points has a specially-selected elliptic curve. These GGT are also applicable in the fourth part of the book where in Chapters 17 and 18 we describe several approaches for iFac of semi-primes. In Chapter 19 a relationship between a *constrained* DLP and iFac is shown. An approach that allows decomposition of large DLP into smaller DLPs is discussed in Chapter 20.

In the fifth part, we provide the description of various problems and related integer algorithms. For instance, we show that some algorithms can be characterized by a set of small integer parameters. As a result, the search for these algorithms can be reduced to the solution of rather simple although computationally-formidable combinatorial problems. However, after they are solved once, these problems lead to the discovery of new algorithms.

The book contains constructive ideas that can be effective in multitude of applications in various business, engineering, financial (EFT), military command/communication/control problems, in deep space exploration and control, in diplomatic exchange, in litigation and other legal actions, in robotic engineering, in remote health care technologies and services in telemedicine (diagnostics, telemonitoring and invasive actions/surgeries, etc.). These ideas can be helpful for studying in depth the computer science

and mathematics of the modern cryptographic and information assurance algorithms.

The book should be of interest to cryptographic experts, communication and network cybersecurity professionals, mathematicians, and students studying theories of information transmission. Results of research, computer experiments and development in these areas that we provide in this book can be instrumental to graduate, postgraduate and PhD students, and their advisors in selecting theses and even PhD topics, semester projects or as guidance for an independent study. The topics and especially the approaches described and analyzed in the book can be instructive for those who are planning to teach advanced-level courses for graduate or PhD students in Computer Science, Electrical Engineering, Telecommunication or Applied Math Departments, as well as for those members of public who have general interest in science and technology. The ideas that we provided and discuss in this book can be helpful to specialists in R&D, who devote their efforts in finding solutions to Big Data challenges in cybersecurity.

Acknowledgments

I express my gratitude to internal and external reviewers for their constructive criticism and suggestions that improved the quality of this book.

Several colleagues, scientists, research collaborators and former undergraduate, graduate and PhD students provided their comments and/or constructive suggestions to various chapters of this book or helped to run computer experiments. Although all remaining errors or ambiguities are mine, I express my deep appreciation to all of them listed here in alphabetic order: W. Amber, D. Chacrabarti, P. Choudhury, H. Cohen, P. Fay, P. Garrett, A. Gerbessiotis, W. Gruver, L. Hars, J. Jones, A. Joux, D. Kanevsky, N. Koblitz, A. Koripella, A. Koval, M. Linderman, X. Ma, M. Marks, S. Medicherla, A. Menezes, W. Miranker, A. Mirajkar, R. Mollin, D. Moody, D. Mozley, D. Murphy, A. Mutovic, S. Naredla, D. Nassimi, D. Nowak, J. Pearson, Y. Polyakov, C. Pomerance, D. Rodik, R. Rubino, J. Runnells, S. Sadik, B. Saraswat, K. Sauraj, J. Scher, I. Semushin, M. Sikorski, K. Skov, R. Statica, B. Tokay, E. Verkhovsky, C. Washington, S. Winograd and the last but not least H. Wozniakowski. And, needless to state that, if I overlooked to mention somebody, I hope for her or his forgiveness.