Computation, Cryptography, and Network Security

Nicholas J. Daras • Michael Th. Rassias
Editors

Computation, Cryptography, and Network Security

Springer

Editors

Nicholas J. Daras
Department of Mathematics
and Engineering
Hellenic Military Academy
Vari Attikis, Greece

Michael Th. Rassias
Department of Mathematics
ETH Zürich
Zürich, Switzerland

ISBN 978-3-319-18274-2 ISBN 978-3-319-18275-9 (eBook)
DOI 10.1007/978-3-319-18275-9

Library of Congress Control Number: 2015945103

Mathematics Subject Classification (2010): 03D25, 11U05, 26D15, 31A10, 45P05, 47G10, 47A07, 44A10, 46E30, 68R10, 94C30

Springer Cham Heidelberg New York Dordrecht London
© Springer International Publishing Switzerland 2015
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

This book entitled *Computation, Cryptography, and Network Security* brings together a broad variety of mathematical methods and theories with several applications from a number of disciplines. It discusses new directions for further inventions in computation, cryptography, and network security.

It is hoped to provide some good understanding of the subject of security in the broadest sense. It consists of papers written by eminent scientists from the international mathematical community, who present important research works in several theories and problems. These contributions focus on both old and new developments of pure and applied mathematics with emphasis to the geometry of the zeros of a polynomial, multivariate Birkhoff interpolation, variational principles in vector spaces, parameterized Yang-Hilbert-type integral inequalities and their operator expressions, operators preserving linear functions, integral estimates for the composition of Green's and bounded operators, asymptotic behavior of orthogonal polynomials on the unit circle, generalized Laplace transform inequalities in multiple weighted Orlicz spaces, and functional equations.

Furthermore, some survey papers are published in this volume, which are particularly useful for a broader audience of readers, particularly in credential technologies, cryptographic schemes, current challenges for IT security with focus on biometry, flaws in the initialization process of stream ciphers, entropy and information measures, information theory, quantum analogues of Hermite-Hadamard type inequalities for generalized convexity, producing fuzzy inclusion and entropy measures, as well as applications on the unstable equilibrium points and system separations in electric power systems, and a supply chain game theory for cybersecurity investments subject to network vulnerability.

We would like to express our deepest thanks to all the contributors of papers who, through their works, participated in this book. We would also wish to acknowledge the superb assistance that the staff of Springer has provided for the publication of this book.

Athens, Greece — Nicholas J. Daras
Princeton, NJ, USA — Michael Th. Rassias

Contents

Transformations of Cryptographic Schemes Through Interpolation Techniques 1
Stamatios-Aggelos N. Alexandropoulos, Gerasimos C. Meletiou, Dimitrios S. Triantafyllou, and Michael N. Vrahatis

Flaws in the Initialisation Process of Stream Ciphers 19
Ali Alhamdan, Harry Bartlett, Ed Dawson, Leonie Simpson, and Kenneth Koon-Ho Wong

Producing Fuzzy Inclusion and Entropy Measures 51
Athanasios C. Bogiatzis and Basil K. Papadopoulos

On Some Recent Results on Asymptotic Behavior of Orthogonal Polynomials on the Unit Circle and Inserting Point Masses 75
Kenier Castillo and Francisco Marcellán

On the Unstable Equilibrium Points and System Separations in Electric Power Systems: A Numerical Study 103
Jinda Cui, Hsiao-Dong Chiang, and Tao Wang

Security and Formation of Network-Centric Operations 123
Nicholas J. Daras

A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security 161
Konstantinos Demertzis and Lazaros Iliadis

Integral Estimates for the Composition of Green's and Bounded Operators 195
Shusen Ding and Yuming Xing

A Survey of Reverse Inequalities for *f*-Divergence Measure in Information Theory 209
S.S. Dragomir

On Geometry of the Zeros of a Polynomial 253
N.K. Govil and Eze R. Nwaeze

Approximation by Durrmeyer Type Operators Preserving Linear Functions 289
Vijay Gupta

Revisiting the Complex Multiplication Method for the Construction of Elliptic Curves 299
Elisavet Konstantinou and Aristides Kontogeorgis

Generalized Laplace Transform Inequalities in Multiple Weighted Orlicz Spaces 319
Jichang Kuang

Threshold Secret Sharing Through Multivariate Birkhoff Interpolation 331
Vasileios E. Markoutis, Gerasimos C. Meletiou, Aphrodite N. Veneti, and Michael N. Vrahatis

Advanced Truncated Differential Attacks Against GOST Block Cipher and Its Variants 351
Theodosis Mourouzis and Nicolas Courtois

A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability 381
Anna Nagurney, Ladimer S. Nagurney, and Shivani Shukla

A Method for Creating Private and Anonymous Digital Territories Using Attribute-Based Credential Technologies 399
Panayotis E. Nastou, Dimitra Nastouli, Panos M. Pardalos, and Yannis C. Stamatiou

Quantum Analogues of Hermite–Hadamard Type Inequalities for Generalized Convexity 413
Muhammad Aslam Noor, Khalida Inayat Noor, and Muhammad Uzair Awan

A Digital Signature Scheme Based on Two Hard Problems 441
Dimitrios Poulakis and Robert Rolland

Randomness in Cryptography 451
Robert Rolland

Current Challenges for IT Security with Focus on Biometry 461
Benjamin Tams, Michael Th. Rassias, and Preda Mihăilescu

Generalizations of Entropy and Information Measures 493
Thomas L. Toulias and Christos P. Kitsos

Maximal and Variational Principles in Vector Spaces 525
Mihai Turinici

All Functions $g{:}\mathbb{N} \to \mathbb{N}$ Which have a Single-Fold Diophantine Representation are Dominated by a Limit-Computable Function $f{:}\mathbb{N} \setminus \{0\} \to \mathbb{N}$ Which is Implemented in *MuPAD* and Whose Computability is an Open Problem 577
Apoloniusz Tyszka

Image Encryption Scheme Based on Non-autonomous Chaotic Systems 591
Christos K. Volos, Ioannis M. Kyprianidis, Ioannis Stouboulos, and Viet-Thanh Pham

Multiple Parameterize Yang-Hilbert-Type Integral Inequalities 613
Bicheng Yang

Parameterized Yang–Hilbert-Type Integral Inequalities and Their Operator Expressions 635
Bicheng Yang and Michael Th. Rassias

A Secure Communication Design Based on the Chaotic Logistic Map: An Experimental Realization Using Arduino Microcontrollers 737
Mauricio Zapateiro De la Hoz, Leonardo Acho, and Yolanda Vidal