

Open Problems in Mathematics and Computational Science

Çetin Kaya Koç
Editor

Open Problems in Mathematics and Computational Science

 Springer

Editor

Çetin Kaya Koç
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA
USA

ISBN 978-3-319-10682-3

ISBN 978-3-319-10683-0 (eBook)

DOI 10.1007/978-3-319-10683-0

Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014957413

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

A selected group of invited speakers and more than 150 students and researchers attended a special conference on September 18–20, 2013, in “Said Halim Pasha Palace” in Istanbul. There had never been a conference of this kind in Turkey, where “open” or “unsolved” problems are discussed, and even in the world there have only been a few examples.

In principle, mathematicians, scientists, and engineers attend conferences to speak about problems they have solved and to “impress” and inform the academic community about their methods and the final solution. It is not generally expected that a researcher would take the stand in a conference to talk about a problem she or he could not (yet) solve. However, all scientific processes start with hypotheses whose ramifications we do not know or problems whose solutions are not clear yet. Either for personal reasons or in accordance with the expectations of scientific conferences and their attendees, researchers tend to push the open/unsolved problems to the back burner and talk about what they have solved, understood, or proved. Still, once in a while (perhaps every 5–10 years), some researchers come together to discuss problems they have not solved yet or problems whose solutions seem rather challenging. Since the 1970s, there have been 7 such conferences.

Therefore, I am very happy that we were able to organize this *Open Problems in Mathematical and Computational Sciences Conference* with support from the Scientific and Technological Research Council (TÜBİTAK) of Turkey.

A large number of young researchers, MSc, and PhD candidates from Turkey, as well as several from neighboring countries, attended the conference. The invited scientists of the conference are among the most prolific mathematical and computational scientists in the world. They come from various countries, demonstrating that science and engineering are culturally very diverse now. The list of countries and number of scientists from each country were a good reminder of this fact: Belgium (2), Brazil (1), Canada (2), China (2), France (3), Germany (2), Japan (1), Norway (1), Romania (1), Turkey (3), and the USA (2).

The Open Problems Conference was held in Said Halim Pasha Palace, one of the most beautiful seaside palaces in Istanbul, whose history goes back at least 150 years and as far as Egypt!

Said Halim Pasha was the son of Mehmet Abdülhalim Pasha who was one of the four sons of Mehmet Ali Pasha from Kavala, the second largest city in Northern Greece. Mehmet Ali Pasha (Muhammad Ali of Egypt) was an Ottoman commander of Albanian origin and is regarded as the founder of modern Egypt because of the dramatic reforms in the military, economic, and cultural spheres he instituted. Said Halim Pasha was born in Cairo in the year 1863 and completed his education in private lessons in Cairo, where he learned Arabic, Persian, English, and French. He studied politics for 5 years in Switzerland. The palace had become the property of Prince Abdülhalim Pasha in the year 1876 and was reconstructed to its current appearance by the travelling architect, Petraki Adamandidis of the Dardanelles. The property was inherited by the nine children of the Abdülhalim Pasha after his death in 1890. After going through several owners, the Said Halim Pasha Palace was restored following a fire in 1995 under the name “Prime Ministry Official Guest House.”

Several peoples’ names need to be mentioned with gratitude, they made both the Open Problems Conference and the Open Problems Book possible.

First of all, I sincerely thank Ronan Nugent for his valuable advice and the Editorial Office of Springer for their help in getting the book published.

On behalf of the invited speakers, I am also sincerely grateful to TÜBİTAK for agreeing with us about the vision of the Open Problems Conference and their subsequent work that produced this book and for providing the financial support. I would also like to thank to Şükran Külekci, İsa Sertkaya, Birnur Ocaklı, Mehmet Sabır Kiraz, and Osmanbey Uzunkol for working around the clock several days before, during, and after the conference.

Santa Barbara, CA, USA

Çetin Kaya Koç

Contents

About Open Problems	1
Çetin Kaya Koç	
The Past, Evolving Present, and Future of the Discrete Logarithm	5
Antoine Joux, Andrew Odlyzko, and Cécile Pierrot	
Isogenies in Theory and Praxis	37
Gerhard Frey	
Another Look at Security Theorems for 1-Key Nested MACs	69
Neal Koblitz and Alfred Menezes	
Non-extendable \mathbb{F}_q-Quadratic Perfect Nonlinear Maps	91
Ferruh Özbudak and Alexander Pott	
Open Problems for Polynomials over Finite Fields and Applications	111
Daniel Panario	
Generating Good Span n Sequences Using Orthogonal Functions in Nonlinear Feedback Shift Registers	127
Kalikinkar Mandal and Guang Gong	
Open Problems on the Cross-correlation of m-Sequences	163
Tor Helleseth	
Open Problems on With-Carry Sequence Generators	181
Andrew Klapper	
Open Problems on Binary Bent Functions	203
Claude Carlet	
On Semi-bent Functions and Related Plateaued Functions Over the Galois Field \mathbb{F}_{2^n}	243
Sihem Mesnager	

True Random Number Generators 275
Mario Stipčević and Çetin Kaya Koç

**How to Sign Paper Contracts? Conjectures and Evidence
Related to Equitable and Efficient Collaborative Task Scheduling** 317
Eric Brier, David Naccache, and Li-yao Xia

Theoretical Parallel Computing Models for GPU Computing 341
Koji Nakano

Membrane Computing: Basics and Frontiers 361
Gheorghe Păun

A Panorama of Post-quantum Cryptography..... 387
Paulo S.L.M. Barreto, Felipe Piazza Biasi, Ricardo Dahab,
Julio César López-Hernández, Eduardo M. de Moraes,
Ana D. Salina de Oliveira, Geovandro C.C.F. Pereira,
and Jefferson E. Ricardini