

# **Mathematics for Industry**

Volume 29

## *Editor-in-Chief*

Masato Wakayama (Kyushu University, Japan)

## **Scientific Board Members**

Robert S. Anderssen (Commonwealth Scientific and Industrial Research Organisation, Australia)

Heinz H. Bauschke (The University of British Columbia, Canada)

Philip Broadbridge (La Trobe University, Australia)

Jin Cheng (Fudan University, China)

Monique Chyba (University of Hawaii at Mānoa, USA)

Georges-Henri Cottet (Joseph Fourier University, France)

José Alberto Cuminato (University of São Paulo, Brazil)

Shin-ichiro Ei (Hokkaido University, Japan)

Yasuhide Fukumoto (Kyushu University, Japan)

Jonathan R.M. Hosking (IBM T.J. Watson Research Center, USA)

Alejandro Jofré (University of Chile, Chile)

Kerry Landman (The University of Melbourne, Australia)

Robert McKibbin (Massey University, New Zealand)

Andrea Parmeggiani (University of Montpellier 2, France)

Jill Pipher (Brown University, USA)

Konrad Polthier (Free University of Berlin, Germany)

Osamu Saeki (Kyushu University, Japan)

Wil Schilders (Eindhoven University of Technology, The Netherlands)

Zuowei Shen (National University of Singapore, Singapore)

Kim-Chuan Toh (National University of Singapore, Singapore)

Evgeny Verbitskiy (Leiden University, The Netherlands)

Nakahiro Yoshida (The University of Tokyo, Japan)

## **Aims & Scope**

The meaning of “Mathematics for Industry” (sometimes abbreviated as MI or MfI) is different from that of “Mathematics in Industry” (or of “Industrial Mathematics”). The latter is restrictive: it tends to be identified with the actual mathematics that specifically arises in the daily management and operation of manufacturing. The former, however, denotes a new research field in mathematics that may serve as a foundation for creating future technologies. This concept was born from the integration and reorganization of pure and applied mathematics in the present day into a fluid and versatile form capable of stimulating awareness of the importance of mathematics in industry, as well as responding to the needs of industrial technologies. The history of this integration and reorganization indicates that this basic idea will someday find increasing utility. Mathematics can be a key technology in modern society.

The series aims to promote this trend by (1) providing comprehensive content on applications of mathematics, especially to industry technologies via various types of scientific research, (2) introducing basic, useful, necessary and crucial knowledge for several applications through concrete subjects, and (3) introducing new research results and developments for applications of mathematics in the real world. These points may provide the basis for opening a new mathematics-oriented technological world and even new research fields of mathematics.

More information about this series at <http://www.springer.com/series/13254>

Tsuyoshi Takagi · Masato Wakayama  
Keisuke Tanaka · Noboru Kunihiro  
Kazufumi Kimoto · Dung Hoang Duong  
Editors

# Mathematical Modelling for Next-Generation Cryptography

CREST Crypto-Math Project

 Springer

*Editors*

Tsuyoshi Takagi  
Kyushu University  
Fukuoka  
Japan

Noboru Kunihiro  
The University of Tokyo  
Kashiwa  
Japan

Masato Wakayama  
Kyushu University  
Fukuoka  
Japan

Kazufumi Kimoto  
University of the Ryukyus  
Nakagami-gun  
Japan

Keisuke Tanaka  
Tokyo Institute of Technology  
Tokyo  
Japan

Dung Hoang Duong  
Institute of Mathematics for Industry  
Kyushu University  
Fukuoka  
Japan

ISSN 2198-350X

Mathematics for Industry

ISBN 978-981-10-5064-0

DOI 10.1007/978-981-10-5065-7

ISSN 2198-3518 (electronic)

ISBN 978-981-10-5065-7 (eBook)

Library of Congress Control Number: 2017943104

© Springer Nature Singapore Pte Ltd. 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

# Preface

The CREST Crypto-Math Project: “Mathematical Modelling for Next-Generation Cryptography” supported by the Japan Science and Technology Agency (JST) aims at constructing mathematical modelling of next-generation cryptography using a wide range of mathematical theories. The goal of the book is to present mathematical background underlying a security modelling of the next-generation cryptography. The book introduces new mathematical results towards strengthening information security, simultaneously making fresh insights and developing the respective areas of mathematics. This project is supported by CREST—a funding program, which is run by the Japan Science and Technology Agency (<https://cryptomath-crest.jp/english>).

There were 19 papers selected for publication. The book is categorized into four parts. Part I is about mathematical cryptography. It covers both topics in post-quantum cryptography, such as multivariate public-key cryptography, code-based cryptography, hash functions based on expander graphs, isogeny-based cryptography and topics in hyperelliptic curve cryptography. Selected areas in mathematical foundation for cryptography including Ramanujan Caley graphs, quantum Rabi models and spectra of group–subgroup pair graphs are discussed in Part II. Part III is devoted to lattices and cryptography with topics ranging from security analysis for post-quantum cryptosystems based on lattices to lattice attacks on RSA cryptosystems. The last part surveys several important cryptographic protocols such as identity-based encryption and fully homomorphic encryption.

The book is suitable for graduate students and researchers. We hope that this book and its individual articles will prove useful for promoting the research on mathematical modelling for post-quantum cryptography.

Fukuoka, Japan  
July 2017

Tsuyoshi Takagi  
Masato Wakayama  
Keisuke Tanaka  
Noboru Kunihiro  
Kazufumi Kimoto  
Dung Hoang Duong

# Contents

<b>Introduction to CREST Crypto-Math Project</b> . . . . .	1
Tsuyoshi Takagi	
<b>Part I Mathematical Cryptography</b>	
<b>Multivariate Public Key Cryptosystems</b> . . . . .	17
Yasufumi Hashimoto	
<b>Code-Based Zero-Knowledge Protocols and Their Applications</b> . . . . .	43
Kirill Morozov	
<b>Hash Functions Based on Ramanujan Graphs</b> . . . . .	63
Hyungrok Jo	
<b>Pairings on Hyperelliptic Curves with Considering Recent Progress on the NFS Algorithms</b> . . . . .	81
Masahiro Ishii	
<b>Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications</b> . . . . .	97
Katsuyuki Takashima	
<b>Part II Mathematics Towards Cryptography</b>	
<b>Spectral Degeneracies in the Asymmetric Quantum Rabi Model</b> . . . . .	117
Cid Reyes-Bustos and Masato Wakayama	
<b>Spectra of Group-Subgroup Pair Graphs</b> . . . . .	139
Kazufumi Kimoto	
<b>Ramanujan Cayley Graphs of the Generalized Quaternion Groups and the Hardy–Littlewood Conjecture</b> . . . . .	159
Yoshinori Yamasaki	

<b>Uniform Random Number Generation and Secret Key Agreement for General Sources by Using Sparse Matrices . . . . .</b>	177
Jun Muramatsu and Shigeki Miyake	
<b>Mathematical Approach for Recovering Secret Key from Its Noisy Version. . . . .</b>	199
Noboru Kunihiro	
<b>Part III Lattices and Cryptography</b>	
<b>Simple Analysis of Key Recovery Attack Against LWE. . . . .</b>	221
Masaya Yasuda	
<b>A Mixed Integer Quadratic Formulation for the Shortest Vector Problem . . . . .</b>	239
Keiji Kimura and Hayato Waki	
<b>On Analysis of Recovering Short Generator Problems via Upper and Lower Bounds of Dirichlet <math>L</math>-Functions: Part 1 . . . . .</b>	257
Shingo Sugiyama	
<b>On Analysis of Recovering Short Generator Problems via Upper and Lower Bounds of Dirichlet <math>L</math>-functions: Part 2 . . . . .</b>	279
Shinya Okumura	
<b>Recent Progress on Coppersmith’s Lattice-Based Method: A Survey . . . . .</b>	297
Yao Lu, Liqiang Peng and Noboru Kunihiro	
<b>Part IV Cryptographic Protocols</b>	
<b>How to Strengthen the Security of Signature Schemes in the Leakage Models: A Survey . . . . .</b>	315
Yuyu Wang and Keisuke Tanaka	
<b>Constructions for the IND-CCA1 Secure Fully Homomorphic Encryption. . . . .</b>	331
Satoshi Yasuda, Fuyuki Kitagawa and Keisuke Tanaka	
<b>A Survey on Identity-Based Encryption from Lattices. . . . .</b>	349
Goichiro Hanaoka and Shota Yamada	
<b>Index . . . . .</b>	367