Mathematics for Industry

Volume 29

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

Masato Wakayama
Kyushu University
Fukuoka
Japan

Keisuke Tanaka
Tokyo Institute of Technology
Tokyo
Japan

Noboru Kunihiro
The University of Tokyo
Kashiwa
Japan

Kazufumi Kimoto
University of the Ryukyus
Nakagami-gun
Japan

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

ISSN 2198-350X ISSN 2198-3518 (electronic)
Mathematics for Industry
ISBN 978-981-10-5064-0 ISBN 978-981-10-5065-7 (eBook)
DOI 10.1007/978-981-10-5065-7

Library of Congress Control Number: 2017943104

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