

# 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

Mathematical Modelling for Next-Generation

Cryptography

CREST Crypto-Math Project

Takagi, T.; Wakayama, M.; Tanaka, K.; Kunihiro, N.;

Kimoto, K.; Duong, D.H. (Eds.)

2018, VIII, 368 p. 23 illus., 6 illus. in color., Hardcover

ISBN: 978-981-10-5064-0