******** CALL FOR PAPERS : CREST BOOK ********

Mathematics, Quantum Theory, and Cryptography

The aim of the book is to present mathematical background underlying a security modelling of the next-generation cryptography. The book will introduce new mathematical results in order to strengthen 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 (JST) (https://cryptomath-crest.jp/english).

This book will contain the selected papers from International Symposium on Mathematics, Quantum Theory, and Cryptography (MQC), which will be held on September 25-27, 2019 in Fukuoka, Japan.

Original research papers/surveys on all technical aspects of mathematical cryptography secure in the era of quantum computers are solicited. The topics include (but are not restricted to): (1) Mathematics and quantum theory for the next-generation cryptography such as: number theory, algebraic geometry, lattice theory, representation theory, multivariate polynomial theory, quantum computation, mathematical physics, and probability theory; (2) Cryptosystems that have the potential to be safe against quantum computers such as: hash-based signature schemes, lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems and quantum cryptographic schemes.

Instructions to authors:
Accepted papers will be published in Springer's “Mathematics for Industry” series available from the website (http://link.springer.com/bookseries/13254). The length of the submission must be at most 15 pages, excluding references and appendices, in a single column format, in 11pt fonts and with reasonable margins. If the submission is accepted, the length of the final version will be at most 20 pages including references and appendices, in the Springer’s format, as in here
https://www.springer.com/gp/authors-editors/book-authors-editors/manuscript-preparation/5636

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. The submission should begin with a title, the authors' names and affiliations, a short abstract, and a list of key words, and its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader.

Authors should submit a paper via email to Yasuhiko Ikematsu <ikematsu@mist.i.u-tokyo.ac.jp>.

Important dates:
Submission Deadline: June 10, 2019
Review Notification: July 22, 2019
First Revision Deadline: August 19, 2019
International Symposium on MQC: September 25-27, 2019
Second Revision Deadline: October 28, 2019
Final Notification: November 25, 2019

Editors:
Tsuyoshi Takagi, University of Tokyo, Japan
Masato Wakayama, Kyushu University, Japan
Keisuke Tanaka, Tokyo Institute of Technology, Japan
Noboru Kunihiro, University of Tokyo, Japan
Kazufumi Kimoto, University of the Ryukyus, Japan

Publicity:
Yasuhiko Ikematsu, University of Tokyo, Japan