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

Mathematical Foundations for Post-Quantum Cryptography

This book presents mathematical foundations for cryptography securely used in the era of quantum computers. In particular, we aim to deepen the basic mathematics of post-quantum cryptography, model the strongest possible attacks such as side-channel attacks, and constructing cryptographic protocols that guarantee security against such attacks. This project is supported by CREST - a funding program, which is run by the Japan Science and Technology Agency (JST) (http://crypto.mist.i.u-tokyo.ac.jp/crest-cryptomath/en/).

The book is planning to be published on July 2024.

Original research papers/surveys on all technical aspects of mathematical cryptography related to the post-quantum cryptography are solicited. The topics include (but are not restricted to): (1)Mathematical background for the post-quantum cryptography such as: number theory, algebraic geometry, lattice theory, representation theory, multivariate polynomial theory, quantum computation and mathematical physics; (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 Momonari Kudo <m-kudo@fit.ac.jp>.

Important dates:
Submission Deadline: November 2nd, 2023
Review Notification: December 7th, 2023
Revision Deadline: January 11th, 2024
Final Notification: February 8th, 2024
Camera-ready version: February 22nd, 2024

Editors:
Tsuyoshi Takagi, The University of Tokyo, Japan
Masato Wakayama, Institute for Fundamental Mathematics, NTT, Japan
Noboru Kunihiro, University of Tsukuba, Japan
Keisuke Tanaka, Tokyo Institute of Technology, Japan
Kazufumi Kimoto, University of the Ryukyus, Japan

Publicity:
Momonari Kudo, Fukuoka Institute of Technology, Japan