Preface

PQCrypto 2016, the 7th International Workshop on Post-Quantum Cryptography, was held in Fukuoka, Japan, during February 24–26, 2016. It was organized in cooperation with the International Association for Cryptologic Research.

The aim of PQCrypto is to serve as a forum for researchers to present results and exchange ideas on the topic of cryptography in the era of large-scale quantum computers. The workshop was preceded by a winter school during February 22–23, 2016.

PQCrypto 2016 has received 42 submissions from 21 countries all over the world. The Program Committee selected 16 papers for publication in the workshop proceedings. The accepted papers deal with multivariate polynomial cryptography, code-based cryptography, lattice-based cryptography, quantum algorithms, post-quantum protocols, and implementations. The program featured four excellent invited talks given by Daniel Bernstein (University of Illinois at Chicago), Ernie Brickell (Intel), Steven Galbraith (University of Auckland), and Masahide Sasaki (Quantum ICT Laboratory, NICT), as well as a hot topic session. The Program Committee selected the work "An Efficient Attack on a Code-Based Signature Scheme" by Aurélie Phesso and Jean-Pierre Tillich for the Best Paper Award of PQCrypto 2016. During the workshop, the National Institute of Standards and Technology (NIST) announced a preliminary plan for the submission and evaluation of quantum-resistant algorithms for potential standardization.

Many people contributed to the success of PQCrypto 2016. I am very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. I am greatly indebted to the general chair, Kouichi Sakurai, for his efforts and overall guidance. I would also like to thank the general co-chairs, Takanori Yasuda and Kirill Morozov, and the local Organizing Committee, Hiroaki Anada, Shinichi Matsumoto, Duong Hoang Dung, Taku Jiromaru, and Emi Watanabe, for their continuous support.

Finally, I would like to express our gratitude to our partners and sponsors: JST CREST, ISIT, ID Quantique, Fukuoka Convention & Vistors Bureau, The Telecommunications Advancement Foundation, and Inoue Foundation for Science. ISIT's contribution to the organization of this workshop is supported by "Strategic Information and Communications R&D Promotion Programme (SCOPE), no. 0159-0016," Ministry of Internal Affairs and Communications, Japan.

February 2016 Tsuyoshi Takagi

http://www.springer.com/978-3-319-29359-2

Post-Quantum Cryptography
7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings
Takagi, T. (Ed.)
2016, X, 267 p. 39 illus. in color., Softcover
ISBN: 978-3-319-29359-2