Preface

PQCrypto 2017, the 8th International Workshop on Post-Quantum Cryptography was held in Utrecht, The Netherlands, during June 26–28, 2017.

The aim of the PQCrypto conference series is to serve as a forum for researchers to present results and exchange ideas on the topic of cryptography in an era with large-scale quantum computers.

PQCrypto 2017 used a two-stage submission process in which authors registered their paper a week before the final submission deadline. The conference received 67 submissions from 24 countries all over the world. After a private review process and an intensive discussion phase with close to 400 discussion comments, the Program Committee selected 23 papers for publication in the proceedings. The accepted papers deal with code-based cryptography, isogeny-based cryptography, lattice-based cryptography, multivariate cryptography, quantum algorithms, and security models.

Along with the 23 contributed presentations, the program featured three excellent invited talks given by Jaya Baloo (KPN), Vadim Lyubashevsky (IBM Research), and Lieven Vandersypen (Technische Universiteit Delft), as well as a hot topic session and a question-and-answer session with the National Institute of Standards and Technology (NIST) about standardization of post-quantum cryptography.

Many people contributed to the success of PQCrypto 2017. We are 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. Special thanks go to Anita Klooster from the Technische Universiteit Eindhoven for taking care of the local arrangements.

June 2017

Tanja Lange
Tsuyoshi Takagi

http://www.springer.com/978-3-319-59878-9

Post-Quantum Cryptography
8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings
Lange, T.; Takagi, T. (Eds.)
2017, XII, 427 p. 34 illus., Softcover
ISBN: 978-3-319-59878-9