

Preface

The 19th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2016) was held March 6–9, 2016 in Taipei (Taiwan). The conference, sponsored by the International Association for Cryptologic Research (IACR), focuses on all technical aspects of public-key cryptography. These proceedings contain 34 papers selected by the Program Committee from 143 submissions. The many high-quality submissions made it easy to build a strong program but also required rejecting good papers. Each submission was judged by at least three reviewers, or four in the case of submissions by Program Committee members. The selection process included one whole month of independent review (each Program Committee member was assigned about 14 papers) followed by five more weeks of discussions. We tried to make the review and discussion system more interactive and used a new feature of the review system that allows Program Committee members to send specific questions to the authors.

We would like to thank the many authors from all over the world for submitting their papers—without them there would not be a conference. We are deeply grateful to the Program Committee for their hard work to ensure that each paper received a thorough and fair review. We gratefully acknowledge the external reviewers listed on the following pages. Our thanks go to Shai Halevi: the committee’s work was tremendously simplified by his submission/review software.

January 2016

Giuseppe Persiano
Bo-Yin Yang

Public-Key Cryptography – PKC 2016

19th IACR International Conference on Practice and
Theory in Public-Key Cryptography, Taipei, Taiwan,
March 6-9, 2016, Proceedings, Part I

Cheng, C.-M.; Chung, K.-M.; Persiano, G.; Yang, B.-Y.
(Eds.)

2016, XIV, 472 p. 46 illus. in color., Softcover

ISBN: 978-3-662-49383-0