

Preface

ASIACRYPT 2017, the 23rd Annual International Conference on Theory and Application of Cryptology and Information Security, was held in Hong Kong, SAR China, during December 3–7, 2017.

The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

ASIACRYPT 2017 received 243 submissions from all over the world. The Program Committee selected 67 papers (from which two were merged) for publication in the proceedings of this conference. The review process was made by the usual double-blind peer review by the Program Committee consisting of 48 leading experts of the field. Each submission was reviewed by at least three reviewers, and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with rebuttal phase. In the first-round review the Program Committee selected the 146 submissions that were considered of value for proceeding to the second round. In the second-round review the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. All the selection process was assisted by 334 external reviewers. These three-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of ASIACRYPT 2017 featured three excellent invited talks. Dustin Moody gave a talk entitled “The Ship Has Sailed: The NIST Post-Quantum Cryptography ‘Competition’,” Wang Huaxiong spoke on “Combinatorics in Information-Theoretic Cryptography,” and Pascal Paillier gave a third talk. The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work “Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems” by Steven D. Galbraith, Christophe Petit, and Javier Silva for the Best Paper Award of ASIACRYPT 2017. Two more papers, “Kummer for Genus One over Prime Order Fields” by Sabyasachi Karati and Palash Sarkar, and “A Subversion-Resistant SNARK” by Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, and Michał Zając were solicited to submit the full versions to the *Journal of Cryptology*. The program chairs selected Takahiro Matsuda and Bart Mennink for the Best PC Member Award.

Many people have contributed to the success of ASIACRYPT 2017. We would like to thank the authors for submitting their research results to the conference. 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. We are greatly indebted to Duncan Wong and Siu Ming Yiu, the general co-chairs, for their efforts and overall organization. We would also like to thank Allen Au, Catherine Chan, Sherman S.M. Chow, Lucas Hui, Zoe Jiang, Xuan Wang, and Jun Zhang, the local

Organizing Committee, for their continuous supports. We thank Duncan Wong and Siu Ming Yiu for expertly organizing and chairing the rump session.

Finally, we thank Shai Halevi for letting us use his nice software for supporting all the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues for handling the editorial process of the proceedings published at Springer LNCS.

December 2017

Tsuyoshi Takagi
Thomas Peyrin

Advances in Cryptology - ASIACRYPT 2017
23rd International Conference on the Theory and
Applications of Cryptology and Information Security,
Hong Kong, China, December 3-7, 2017, Proceedings,
Part I

Takagi, T.; Peyrin, Th. (Eds.)

2017, XXVI, 813 p. 121 illus., Softcover

ISBN: 978-3-319-70693-1