

Preface

ASIACRYPT 2015, the 21st Annual International Conference on Theory and Application of Cryptology and Information Security, was held on the city campus of the University of Auckland, New Zealand, from November 29 to December 3, 2015. The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

The conference received 251 submissions from all over the world. The program included 64 papers selected from these submissions by a Program Committee (PC) comprising 43 leading experts of the field. In order to accommodate as many high-quality submissions as possible, the conference ran in two parallel sessions, and these two-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 selection of the papers was made through the usual double-blind review process. Each submission was assigned three reviewers and submissions by PC members were assigned five reviewers. The selection process was assisted by a total of 339 external reviewers. Following the individual review phase, the selection process involved an extensive discussion phase.

This year, the conference featured three invited talks. Phillip Rogaway gave the 2015 IACR Distinguished Lecture on “The Moral Character of Cryptographic Work,” Gilles Barthe gave a talk on “Computer-Aided Cryptography: Status and Perspectives,” and Masayuki Abe spoke on “Structure-Preserving Cryptography.” The proceedings contain the abstracts of these talks. The conference also featured a traditional rump session that contained short presentations on the latest research results of the field.

The best paper award was decided based on a vote by the PC members, and it was given to “Improved Security Proofs in Lattice-Based Cryptography: Using the Rényi Divergence Rather than the Statistical Distance” by Shi Bai, Adeline Langlois, Tancrede Lepoint, Damien Stehlé, and Ron Steinfeld. Two more papers, “Key-Recovery Attacks on ASASA” by Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman, and “The Tower Number Field Sieve” by Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung, were solicited to submit full versions to the *Journal of Cryptology*.

ASIACRYPT 2015 was made possible by the contributions of many people. We would like to thank the authors for submitting their research results to the conference. We are deeply grateful to all the PC members and all the external reviewers for their hard work to determine the program of the conference. We sincerely thank Steven Galbraith, the general chair of the conference, and the members of the local Organizing Committee for handling all the organizational work of the conference. We also thank Nigel Smart for organizing and chairing the rump session.

We thank Shai Halevi for setting up and letting us use the IACR conference management software. Springer published the two-volume proceedings and made these

available at the conference. We thank Alfred Hofmann, Anna Kramer, and their colleagues for handling the editorial process. Last but not least, we thank the speakers, session chairs, and all the participants for coming to Auckland and contributing to ASIACRYPT 2015.

December 2015

Tetsu Iwata
Jung Hee Cheon

Advances in Cryptology -- ASIACRYPT 2015
21st International Conference on the Theory and
Application of Cryptology and Information
Security, Auckland, New Zealand, November 29 --
December 3, 2015, Proceedings, Part I
Iwata, T.; Cheon, J.H. (Eds.)
2015, XXV, 810 p. 93 illus., Softcover
ISBN: 978-3-662-48796-9