Preface

The 15th International Conference on Applied Cryptography and Network Security (ACNS2017) was held in Kanazawa, Japan, during July 10–12, 2017. The previous conferences in the ACNS series were successfully held in Kunming, China (2003), Yellow Mountain, China (2004), New York, USA (2005), Singapore (2006), Zhuhai, China (2007), New York, USA (2008), Paris, France (2009), Beijing, China (2010), Malaga, Spain (2011), Singapore (2012), Banff, Canada (2013), Lausanne, Switzerland (2014), New York, USA (2015), and London, UK (2016).

ACNS is an annual conference focusing on innovative research and current developments that advance the areas of applied cryptography, cyber security, and privacy. Academic research with high relevance to real-world problems as well as developments in industrial and technical frontiers fall within the scope of the conference.

This year we have received 149 submissions from 34 different countries. Each submission was reviewed by 3.7 Program Committee members on average. Papers submitted by Program Committee members received on average 4.4 reviews. The committee decided to accept 34 regular papers. The broad range of areas covered by the high-quality papers accepted for ACNS 2107 attests very much to the fulfillment of the conference goals.

The program included two invited talks given by Dr. Karthikeyan Bhargavan (Inria Paris) and Prof. Doug Tygar (UC Berkeley).

The decisions of the best student paper award was based on a vote among the Program Committee members. To be eligible for selection, the primary author of the paper has to be a full-time student who is present at the conference. The winner was Carlos Aguilar-Melchor, Martin Albrecht, and Thomas Ricosset from Université de Toulouse, Toulouse, France, Royal Holloway, University of London, UK, and Thales Communications & Security, Gennevilliers, France. The title of the paper is “Sampling From Arbitrary Centered Discrete Gaussians For Lattice-Based Cryptography.”

We are very grateful to our supporters and sponsors. The conference was co-organized by Osaka University, Japan Advanced Institute of Science and Technology (JAIST), and the Information-technology Promotion Agency (IPA); it was supported by the Committee on Information and Communication System Security (ICSS), IEICE, Japan, the Technical Committee on Information Security (ISEC), IEICE, Japan, and the Special Interest Group on Computer SECurity (CSEC) of IPSJ, Japan; it and was co-sponsored by the National Institute of Information and Communications Technology (NICT) International Exchange Program, Mitsubishi Electric Corporation, Support Center for Advanced Telecommunications Technology Research (SCAT), Foundation Microsoft Corporation, Fujitsu Hokuriku Systems Limited, Nippon Telegraph and Telephone Corporation (NTT), and Hokuriku Telecommunication Network Co., Inc.

We would like to thank the authors for submitting their papers to the conference. The selection of the papers was a challenging and dedicated task, and we are deeply grateful to the 48 Program Committee members and the external reviewers for their reviews and discussions. We also would like to thank EasyChair for providing a user-friendly interface for us to manage all submissions and proceedings files. Finally, we would like to thank the general chair, Prof. Hiroaki Kikuchi, and the members of the local Organizing Committee.

July 2017

Dieter Gollmann
Atsuko Miyaji

http://www.springer.com/978-3-319-61203-4

Applied Cryptography and Network Security
15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings
Gollmann, D.; Miyaji, A.; Kikuchi, H. (Eds.)
2017, XVI, 710 p. 167 illus., Softcover
ISBN: 978-3-319-61203-4