

Preface

The 9th International Conference on Provable Security (ProvSec 2015) was held in Kanazawa, November 24–26, 2015. The previous ProvSec series were successfully held in Wollongong, Australia (2007), Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010), Xi'an, China (2011), Chengdu, China (2012), Malacca, Malaysia (2013) and Hong Kong, China (2014). This was the first ProvSec held in Japan.

The main goal of ProvSec as a conference is to promote research on all aspects of provable security for cryptographic primitives or protocols, including but not limited to the following areas: asymmetric provably secure cryptography; cryptographic primitives; lattice-based cryptography and security reductions, leakage-resilient cryptography, pairing-based provably secure cryptography; privacy and anonymity technologies; provable secure block ciphers and hash functions; secure cryptographic protocols and applications; security notions, approaches, and paradigms; and steganography and steganalysis. This year we received 60 submissions from 23 different countries. Each submission was reviewed by at least three, and on average four, Program Committee members. Papers submitted by Program Committee members received at least four, and on the average 4.4, reviews. The committee decided to accept 19 regular papers and seven short papers. The broad range of areas covered by the high-quality accepted papers in the current edition attests to the fulfillment of that goal.

The program included three invited talks, given by Prof. Sanjam Garg (University of California, Berkeley) titled “New Advances in Secure RAM Computation,” Prof. Phillip Rogaway (University of California, Davis) titled “Advances in Authenticated Encryption,” and Prof. Serge Vaudenay (École Polytechnique Fédérale de Lausanne) titled “On Privacy for RFID”.

The decision on the best paper award was based on a vote among the Program Committee members. The best paper award was conferred upon the paper “From Stateful Hardware to Resettable Hardware Using Symmetric Assumptions” authored by Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade, and Tobias Nilges. In addition, the Program Committee selected the best student paper. To be eligible for selection, the primary author of the paper has to be a full-time student who gives a presentation at the conference. The winner was Bei Liang from the University of Chinese Academy of Sciences, Beijing, China, for the paper “Constrained Verifiable Random Functions from Indistinguishability Obfuscation.”

We are very grateful to our supporters and sponsors. The conference was co-organized by the Information-technology Promotion Agency, Japan (IPA) and Japan Advanced Institute of Science and Technology (JAIST), it was supported by the Technical 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, and was co-sponsored by Mitsubishi Electric, National Institute of Information and

Communications Technology (NICT), Support Center for Advanced Telecommunications Technology Research (SCAT), and Nippon Telegraph and Telephone Corporation (NTT).

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 35 Program Committee members and the external reviewers for their reviews and discussions. We would also 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, Dr. Tatsuaki Okamoto, and we the members of the local Organizing Committee.

September 2015

Man-Ho Au
Atsuko Miyaji

Provable Security

9th International Conference, ProvSec 2015, Kanazawa,
Japan, November 24-26, 2015, Proceedings

Au, M.-H.; Miyaji, A. (Eds.)

2015, XIX, 504 p. 65 illus. in color., Softcover

ISBN: 978-3-319-26058-7