

Preface

The 10th International Conference on Provable Security (ProvSec 2016) was held in Nanjing, P.R. China, November 10–11, 2016. The conference was organized by Nanjing University of Finance and Economics.

The conference program consisted of two invited talks and 23 contributed papers. We would like to express our special thanks to the distinguished keynote speakers, Colin Boyd from the Norwegian University of Science and Technology and Jens Groth from University College London, who gave very enlightening talks.

Out of 79 submissions from 16 countries, 23 papers were selected, presented at the conference, and are included in these proceedings. The accepted papers cover a range of topics in the field of provable security research, including attribute/role-based cryptography, data in cloud, searchable encryption, key management, encryption, leakage analysis, and homomorphic encryption.

The success of this event depended critically on the help and hard work of many people, whose help we gratefully acknowledge. First, we heartily thank the Program Committee and the additional reviewers, listed on the following pages, for their careful and thorough reviews. Most of the papers were reviewed by at least three people, and many by four or five. Significant time was spent discussing the papers. Thanks must also go to the hard-working shepherds for their guidance and helpful advice on improving a number of papers. We also thank the general chair for the excellent organization of the conference.

We also sincerely thank the authors of all submitted papers. We further thank the authors of accepted papers for revising papers according to the various reviewer suggestions and for returning the source files in good time. The revised versions were not checked by the Program Committee, and so authors bear final responsibility for their contents. We would also like to thank the Steering Committee and local Organizing Committee.

Thanks are due to the staff at Springer for their help in producing the proceedings. We further thank the developers and maintainers of the EasyChair software, which greatly helped simplify the submission and review process.

November 2016

Liqun Chen
Jinguang Han

Provable Security

10th International Conference, ProvSec 2016, Nanjing,
China, November 10-11, 2016, Proceedings

Chen, L.; Han, J. (Eds.)

2016, XIII, 394 p. 34 illus., Softcover

ISBN: 978-3-319-47421-2