

Preface

This volume contains the papers accepted for presentation at the 6th International Conference on Security, Privacy, and Applied Cryptography Engineering 2016 (SPACE 2016), held during December 14–18, 2016, at the C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS), University of Hyderabad, India. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is indeed a very challenging field, requiring expertise from diverse domains, ranging from mathematics to solid-state circuit design.

This year we received 54 submissions from about 20 countries, out of which, after an extensive review process, 16 papers were accepted for presentation at the conference, and one shorter paper was accepted for short presentation. The submissions were evaluated based on their significance, novelty, technical quality, and relevance to the SPACE conference. The submissions were reviewed in a double-blind mode by at least three members of the 35-member Program Committee (one more if at least one of the authors was member of the Program Committee). The Program Committee was aided by 36 additional reviewers. The Program Committee meetings were held electronically, with intensive discussions.

The program also included eight invited talks and four tutorials on several aspects of applied cryptology, delivered by world-renowned researchers: Lejla Batina, Shivam Bhasin, Swarup Bhunia, Craig Costello, Joan Daemen, Christian Grothoff, Debdeep Mukhopadhyay, Emmanuel Prouff, François-Xavier Standaert, and Ingrid Verbauwhede. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules.

Like its previous editions, SPACE 2016 was organized in co-operation with the International Association for Cryptologic Research (IACR). We are thankful to AIMSCS for being the gracious host of SPACE 2016.

There is a long list of volunteers who invested their time and energy to put together the conference, and who deserve accolades for their efforts. We are grateful to all the members of the Program Committee and the additional reviewers for all their hard work in the evaluation of the submitted papers. We thank Cool Press Ltd., owner of the EasyChair conference management system, for allowing us to use it for SPACE 2016, which was a great help. We also sincerely thank our publisher Springer for agreeing to continue to publish the SPACE proceedings as a volume in the *Lecture Notes in Computer Science* (LNCS) series. We are further very grateful to the members of the local Organizing Committee, including Sahana Subbarao, for their assistance to Vishal Saraswat in ensuring the smooth organization of the conference. Special thanks to our general chairs, Arun Kumar, Arun Agarwal and Sitaram Chamarty, for their constant support and encouragement.

Last, but certainly not least, our sincere thanks go to all the authors who submitted papers to SPACE 2016, and to all the attendees. The conference was made possible by you, and the proceedings are dedicated to you. We sincerely hope you find the program proceedings stimulating and inspiring.

December 2016

Claude Carlet
M. Anwar Hasan
Vishal Saraswat

Security, Privacy, and Applied Cryptography Engineering
6th International Conference, SPACE 2016, Hyderabad,
India, December 14-18, 2016, Proceedings
Carlet, C.; Hasan, M.A.; Saraswat, V. (Eds.)
2016, XXIII, 420 p. 139 illus., Softcover
ISBN: 978-3-319-49444-9