

Preface

This volume contains the papers accepted for presentation at the 7th International Conference on Security, Privacy, and Applied Cryptography Engineering 2017 (SPACE 2017), held during December 13–17, 2017, at the Don Bosco College of Engineering, Goa, 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 49 submissions from about eight different countries, out of which, after an extensive review process, 13 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 36-member Program Committee (one more if at least one of the authors was member of the Program Committee). The Program Committee was aided by 50 additional reviewers. The Program Committee meetings were held electronically, with intensive discussions.

The program also included seven invited talks and four tutorials on several aspects of applied cryptology, delivered by world-renowned researchers: Asaf Ashkenazi, Shivam Bhasin, Jean-Luc Danger, Thomas Eisenbarth, Harry Halpin, Mike Hamburg, Gary Kenworthy, Victor Lomne, Axel Poschmann, Karim Tobich, Ingrid Verbauwhede, and Yuval Yarom. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. Like its previous editions, SPACE 2017 was organized in co-operation with the International Association for Cryptologic Research (IACR). We are thankful to Don Bosco College of Engineering for being the gracious host of SPACE 2017.

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 2017, which was a great help. We 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 grateful to the local Organizing Committee, especially to the organizing chair, Roseline Fernandes, who invested a lot effort for the conference to run smoothly. We are further very grateful to Vishal Saraswat, program chair of SPACE 2016, for his guidance and active support toward organizing SPACE 2017. Special thanks to our general chairs, Rev. Fr. Kinley D'Cruz, Neena Panandikar, and Sandeep Shukla, for their support and encouragement. Our sincere gratitude to Deb-deep Mukhopadhyay, Veezhinathan Kamakoti, and Sanjay Burman for being

constantly involved in SPACE since its very inception and responsible for SPACE reaching its current status.

Last, but certainly not least, our sincere thanks go to all the authors who submitted papers to SPACE 2017, and to all the attendees. The conference is made possible by you, and it is dedicated to you. We sincerely hope you find the proceedings stimulating and inspiring.

October 2017

Sk Subidh Ali
Jean-Luc Danger
Thomas Eisenbarth

Security, Privacy, and Applied Cryptography Engineering
7th International Conference, SPACE 2017, Goa, India,
December 13-17, 2017, Proceedings
Ali, S.S.; Danger, J.-L.; Eisenbarth, Th. (Eds.)
2017, XXIV, 295 p. 55 illus., Softcover
ISBN: 978-3-319-71500-1