Preface

It gives us immense pleasure to present the proceedings of the Fifth International Conference on Security, Privacy, and Applied Cryptography Engineering 2015 (SPACE 2015), held during October 3–7, 2015, at the Malaviya National Institute of Technology (MNIT), Jaipur, Rajasthan, 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 the expertise from diverse domains, ranging from mathematics to solid-state circuit design.

This year we received 57 submissions from 17 different countries, out of which 17 papers were accepted for presentation at the conference after an extensive review process. 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 Program Committee. The Program Committee was aided by 28 sub-reviewers. The Program Committee meetings were held electronically, with intensive discussions over a period of almost two weeks.

The program also included 9 invited talks and tutorials on several aspects of applied cryptology, delivered by world-renowned researchers: Jacob Appelbaum (Eindhoven University of Technology/The Tor Project), Daniel Bernstein (Eindhoven University of Technology/University of Illinois at Chicago), Claude Carlet (University of Paris 8), Trent Jaeger (The Pennsylvania State University) Rafael Boix Carpi & Vishwas Raj Jain (Riscure BV), Tanja Lange (Eindhoven University of Technology), Sri Parameswaran (University of New South Wales), Sandeep Shukla (Indian Institute of Technology Kanpur), Graham Steel (Inria), and Petr Švenda (Masaryk University), We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules.

Over the last five years, the SPACE conference has grown considerably, especially with respect to its appeal to the international applied security research community. SPACE 2015 was built upon the strong foundation laid down by dedicated academicians and industry professionals. In particular, we would like to thank the Program Chairs of the previous editions: Debdeep Mukhopadhyay, Benedikt Gierlichs, Sylvain Guilley, Andrey Bodganov, Somitra Sanadhya, Michael Tunstall, Marc Joye, Patrick Schaumont, and Vashek Matyas. Because of their efforts, SPACE is already in the "must submit" list of many leading researchers of applied security around the world. It still has a long way to go, but it is moving in the right direction.

Like its previous editions, SPACE 2015 was organized in co-operation with the International Association for Cryptologic Research (IACR). We are thankful to the Malaviya National Institute of Technology (MNIT) for being the gracious hosts of SPACE 2015. The conference was sponsored by the Defence Research

and Development Organisation (DRDO), under the auspices of the Ministry of Defence (Govt. of India). The other sponsors are ISEA and MNIT. We would like to thank them for their generous financial support, which has helped us to avoid steep hikes in the registration fees in comparison with previous editions, thus ensuring wider participation, particularly from the student community of India.

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 sub-reviewers for all their hard work in the evaluation of the submitted papers. Our heartiest thanks to Cool Press Ltd., owners of the EasyChair conference management system, for allowing us to use it for SPACE 2015. EasyChair was largely instrumental in the timely and smooth operation needed for managing such an international event. 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 all the members of the Local Organizing Committee for their assistance in ensuring the smooth organization of the conference, especially M.S. Gaur, M.C. Govil, R.B. Battula, V. Laxmi, M. Tripathi, L. Bhargava, E.S. Pilli, and S. Vipparthi from MNIT Jaipur. Special thanks to our General Chairs, Adrian Perrig and Debdeep Mukhopadhyay, for their constant support and encouragement. We would also like to thank Vashek Matyas for managing the tutorials and the pre-conference workshop. We would like to thank Swarup Bhunia and R.B. Battula for taking on the extremely important role of Publicity Chairs. No words can express our sincere gratitude to Debdeep Mukhopadhyay for being constantly involved in SPACE since its very inception, and being the person most responsible for SPACE reaching its current status. We thank Durga Prasad for his commendable job in maintaining the website for SPACE 2015, and timely updates.

Last, but certainly not least, our sincere thanks go to all the authors who submitted papers to SPACE 2015, and to all the attendees. The conference is made possible by you, and it is dedicated to you. We sincerely hope you find the program stimulating and inspiring.

October 2015

Rajat Subhra Chakraborty
Peter Schwabe
Jon Solworth

http://www.springer.com/978-3-319-24125-8

Security, Privacy, and Applied Cryptography Engineering
5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings
Chakraborty, R.S.; Schwabe, P.; Solworth, J. (Eds.)
2015, XVIII, 373 p. 88 illus. in color., Softcover
ISBN: 978-3-319-24125-8