

Preface

ICITS 2013, the 7th International Conference on Information Theoretic Security, was held in Singapore during November 28–30, 2013. The conference took place on the One-North Campus of the Nanyang Technological University. The general chairs of the conference were Frédérique Oggier and Miklos Santha.

Information theoretic cryptography analyzes the existence and efficiency of cryptographic schemes whose security is not based on computational hardness assumptions. This research topic is connected to several areas of mathematics such as probability and information theory, algebra and algebraic geometry, combinatorics, coding theory and quantum information processing, among others.

Two different kinds of submissions were solicited for ICITS 2013. Only original research work could be submitted to the *Conference Track*, while submissions to the *Workshop Track* could consist of research work that had been recently published or submitted to other venues. Every submission was considered only for one track, chosen by the authors. The two-track format was initiated in ICITS 2012, the previous edition of the conference, and it has proved to be very successful in bringing together researchers from information theory, cryptography, and quantum computing, communities with different publication traditions.

The Program Committee received a total of 49 submissions, of which 14 were accepted for the Conference Track and 10 for the Workshop Track. All submitted papers were revised by the Program Committee, with the help in some cases of external reviewers. These proceedings contain the accepted papers for the Conference Track. The accepted works for the Workshop Track were presented at the conference but do not appear in this volume. The list of the contributions in the Workshop Track is given before the Table of Contents.

In addition to the contributed presentations, the program was completed with three invited talks:

- “*Multi-Linear Secret Sharing Schemes*,” by Amos Beimel, Ben-Gurion University, Israel
- “*Entropic Uncertainty Relations and Their Applications in Quantum Cryptography*” by Marco Tomamichel, Centre for Quantum Technologies (CQT), Singapore
- “*New Results on Percolation Through Topological Quantum Error Correcting Codes*,” by Gilles Zémor, Université de Bordeaux, France

Many people have contributed to the success of ICITS 2013. First of all, I thank all authors of submitted papers for choosing ICITS 2013 to disseminate their work. Many thanks to the members of the Program Committee. It was a pleasure to collaborate with such a team of motivated, talented, and hardworking scientists to put together the program of the conference. Reviewing and selecting the papers was a difficult task that required a lot of their time and efforts. I also thank the external reviewers for assisting the Program Committee in the reviewing process. I thank Adam Smith for his very

good advice and for sharing his experience as program chair of ICITS 2012. Special thanks to the general chairs, Frédérique Oggier and Miklos Santha, for their invaluable work in organizing the conference, and many thanks to all people who assisted them in that challenging task: Noelle Chen from MAS General Office, NTU, Helen Chen and Nicholas Tee from SPMS IT support, NTU, Nweni Myint Aung from CITS, NTU, and Evon Tan from CQT, NUS.

November 2013

Carles Padró

Information Theoretic Security

7th International Conference, ICITS 2013, Singapore,

November 28-30, 2013, Proceedings

Padró, C. (Ed.)

2014, XII, 259 p. 29 illus., Softcover

ISBN: 978-3-319-04267-1