Preface

ICITS 2015, the 8th International Conference on Information-Theoretic Security, was held in Lugano, Ticino, Switzerland, during May 2–5, 2015. The conference took place on the campus of Università della Svizzera italiana (USI) in Molino Nuovo, Lugano. The General and Program Co-chairs were Anja Lehmann (IBM Research – Zurich) and Stefan Wolf (USI Lugano).

The scope of ICITS connects the fields of cryptography, information theory, and quantum physics. More specifically, methods are studied that achieve cryptographic security without computational assumptions, or as "post-quantum schemes" which employ techniques from information theory, *e.g.*, coding.

ICITS 2015 had two tracks, a conference and a workshop track: Conference-track articles also appear in the proceedings, whereas workshop-track contributions were only presented on-site with a talk. This two-track format, which was started with ICITS 2012, has the advantage to promote bringing together researchers from various areas, such as information theory, cryptography, and quantum computing, which have different publication traditions.

There were 57 submitted papers, 48 to the conference track and 9 to the workshop track. In total, 23 submissions were accepted, 17 for the conference track and 6 for the workshop track. All submissions were reviewed by at least 3 (conference track) or 2 (workshop track) members of the Program Committee, who sometimes were assisted by external reviewers. These proceedings contain the accepted papers for the conference track. A full list of the workshop-track papers is given before the table of contents.

The conference program also featured five invited talks:

- "New Developments in Relativistic Quantum Cryptography" by *Adrian Kent*, University of Cambridge, UK
- "Tamper and Leakage Resilient von Neumann Architectures from Continuous Non-Malleable Codes" by *Jesper Buus Nielsen*, Aarhus University, Denmark. (Abstract included in this volume.)
- "Classical Uses of Quantum Complementarity: Leakage Resilient Computation and Semantically-Secure Communication" by *Joseph Renes*, ETH Zurich, Switzerland.
- "Tamper-Detection and Non-Malleable Codes" by *Daniel Wichs*, Northeastern University, USA.
- "Reflections on Quantum Data Hiding" by *Andreas Winter*, Universitat Autònoma de Barcelona, Spain.

First of all, we thank the Steering Committee of ICITS, and in particular Yvo Desmedt as well as Rei Safavi-Naini, for their trust and support. We would like to thank all the people who have contributed to the success of ICITS 2015. First, we thank the authors for submitting their work to our conference. It was a great pleasure to work with such a motivated and professional Program Committee. We would like to thank all

PC members for their contribution, and also thank the external reviewers who assisted the Program Committee during the reviewing process. We are grateful to the General and Program Chairs of previous editions of ICITS for their advice and assistance, in particular Frédérique Oggier, Carles Padro, Adam Smith, and Jürg Wullschleger. We also thank Jan Camenisch for his advice on various questions on how to run a conference. We are indebted to Ämin Baumeler for his most generous support, for instance, in producing these proceedings. Diana Corica was helping us with various administrative matters that pop-up in the organization of such an event; grazie mille! We thank a very motivated and competent Local Organization Committee for their precious help, namely Ämin Baumeler, Diana Corica, Helen Ebbe, Arne Hansen, Elisa Larghi, and Benno Salwey. Finally, ICITS 2015 would not have been possible without the generous financial support we received. In particular, we are most grateful to Albino Zgraggen and Klaus Ensslin. Our sponsors were the Università della Svizzera italiana (USI), the NCCR "Quantum Science and Technology" (QSIT), and the City of Lugano.

February 2015

Anja Lehmann
Stefan Wolf

http://www.springer.com/978-3-319-17469-3

Information Theoretic Security
8th International Conference, ICITS 2015, Lugano, Switzerland, May 2-5, 2015. Proceedings
Lehmann, A.; Wolf, S. (Eds.)
2015, XIV, 297 p. 29 illus., Softcover
ISBN: 978-3-319-17469-3