Lecture Notes in Computer Science 8317

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

For further volumes:
http://www.springer.com/series/7410

Carles Padró (Ed.)

Information Theoretic Security

7th International Conference, ICITS 2013
Singapore, November 28–30, 2013
Proceedings

Springer

Editor
Carles Padró
Nanyang Technological University
Singapore
Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
ISBN 978-3-319-04267-1 ISBN 978-3-319-04268-8 (eBook)
DOI 10.1007/978-3-319-04268-8
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013957942

CR Subject Classification (1998): K.6.5, E.3, E.4, K.4.4, F.2.1

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

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

ICITS 2013

The 7th International Conference on Information Theoretic Security
Singapore, November 28–30, 2013

General Chairs

Frédérique Oggier	Nanyang Technological University, Singapore
Miklos Santha	CNRS, Paris, France; CQT, Singapore

Program Chair

Carles Padró	Nanyang Technological University, Singapore

Program Committee

Simon R. Blackburn	Royal Holloway University of London, UK
Matthieu Bloch	Georgia Tech, USA
Ignacio Cascudo	CWI Amsterdam, The Netherlands
László Csirmaz	CEU Budapest, Hungary
Stefan Dziembowski	University of Warsaw, Poland
Serge Fehr	CWI Amsterdam, The Netherlands
Juan Garay	AT&T Labs – Research, USA
Masahito Hayashi	Nagoya University, Japan
Javier Herranz	Universitat Politècnica de Catalunya, Spain
Iordanis Kerenidis	CNRS, Université Paris Diderot, France
Lifeng Lai	Worcester Polytechnic Institute, USA
Leonid Reyzin	Boston University, USA
Tamir Tassa	The Open University of Israel
Stephanie Wehner	CQT and NUS, Singapore
Chaoping Xing	Nanyang Technological University, Singapore

ICITS Steering Committee

Carlo Blundo	University of Salerno, Italy
Ronald Cramer	CWI and Leiden University, The Netherlands
Yvo Desmedt, Chair	University College London, UK
Hideki Imai	University of Tokyo, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Ueli Maurer	ETH Zürich, Switzerland
C. Pandu Rangan	Indian Institute of Technology, Madras, India

Rei Safavi-Naini	University of Calgary, Canada
Moti Yung	Google and Columbia University, USA
Yulian Zheng	University of North Carolina, USA

Additional Reviewers

Emmanuel Abbe
Adi Akavia
Frederik Armknecht
Salman Beigi
Yu Cai
Antonio Campello
Nishanth Chandran
Robbert de Haan
Nadia El Mrabet
Alex Escala
Omar Fawzi
Atsushi Fujioka
Fabian Furrer
Steven Galbraith
Tanvirul Islam
Jedrzej Kaniewski
Bhavana Kanukurthi
Takeshi Koshiba
Ranjit Kumaresan
Adriana López-Alt
Steve Lu
Sebastià Martín
Ryutaroh Matsumoto
Diego Mirandola
Pritam Mukherjee
Siaw-Lynn Ng
Christopher Portmann
Christian Schaffner
Björn Tackmann
Yevgeniy Vahlis
Yu Yu
Mark Zhandry

Sponsors

Lee Foundation, Singapore
CryptoWorks21, Institute for Quantum Computing, University of Waterloo, Canada
Centre for Quantum Technologies, Singapore

Lee Foundation

CryptoWorks21

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Workshop Track Presentations

1. One-Sided Device Independence of BB84 Via Monogamy-of-Entanglement Game
   Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, Stephanie Wehner
2. Secret Key Agreement Over a Lossy Optical Channel with a Passive Quantum Eavesdropper: Capacity Bounds and New Explicit Protocols
   Saikat Guha, Masahiro Takeoka, Hari Krovi, Mark M. Wilde, Cosmo Lupo
3. Efficient One-Way Secret-Key Agreement and Private Channel Coding Via Polarization
   David Sutter, Joseph M. Renes and Renato Renner
4. Composable Security of Measuring—Alice Blind Quantum Computation
   Tomoyuki Morimae, Takeshi Koshiba
5. Quantum Enigma Machines and the Locking Capacity of a Quantum Channel
   Saikat Guha, Patrick Hayden, Hari Krovi, Seth Lloyd, Cosmo Lupo, Jeffrey H. Shapiro, Masahiro Takeoka, Mark M. Wilde
6. Oblivious Transfer, the CHSH Game, and Quantum Encodings
   André Chailloux, Iordanis Kerenidis, Jamie Sikora
7. Non-Asymptotic Analysis of Privacy Amplification for Markov Chains
   Masahito Hayashi, Shun Watanabe
8. A Secret Images Sharing Scheme Using the Two-Variable One-Way Functions Approach with Public Values' Hiding
   Todorka Alexandrova
9. Security Analysis for a Relativistic Bit Commitment Experiment
   Jedrzej Kaniewski, Marco Tomamichel, Stephanie Wehner
10. Reference Frame Agreement in Quantum Networks
    Tanvirul Islam, Loïck Magnin, Brandon Sorg, Stephanie Wehner

Contents