ICITS 2012 was the 6th International Conference of Information-theoretic Security, held at the Université de Montréal in Montreal, Quebec, Canada, during August 15–17, 2012. ICITS 2012 was held in cooperation with the International Association for Cryptologic Research (IACR). The General Chair of the conference was Jürg Wullschleger. He was helped by two local Co-chairs, Claude Crépeau and Alain Tapp.

The Program Committee, consisting of 14 members, received 46 submissions to two tracks. Twenty-two papers were ultimately accepted, 11 from each track. The quality of the submissions to both tracks was high, making the selection process challenging.

The two-track format was new to ICITS this year, and represented an experiment in bringing together researchers from three communities — information theory, cryptography, quantum computing — with very different publication cultures. Submissions to both tracks were reviewed by the committee, and in some cases external reviewers, to assess their quality and suitability. The two tracks differed in how accepted submissions were handled. The first, “conference”, track was set up as a traditional computer science conference: submissions had to be original, and revised versions of the 11 accepted papers appear in this volume. (Revisions were not checked as to their contents, and the authors bear full responsibility for the contents of their papers.)

In contrast, papers accepted to the second, “workshop”, track do not appear in these proceedings except, at the discretion of the authors, as one-page abstracts (authors of seven of the 11 papers decided to contribute abstracts). Workshop-track papers represent recently published or as-yet unpublished research. A full list of the workshop-track papers presented at the conference appears before the table of contents.

The goal of the two-track format was to encourage participation from researchers from communities where a conference publication may preclude publication in a top journal, and to draw participants who normally publish in other conferences (CRYPTO and ISIT, for example). I believe that in this respect the format was very successful.

Finally, I note that it was up to authors to decide which track they would submit to—each paper was only considered for one track—and the same review process applied to papers from both tracks.

In addition to the 22 contributed presentations, there were seven invited talks:

- “Reconstruction of a Shared Secret in the Presence of Faults,” by Serge Fehr of CWI Amsterdam
- “Timing Side Channels: Quantifying and Mitigating the Threat,” by Negar Kiyavash of the University of Illinois at Urbana-Champaign
− “Non-malleable Extractors, Non-malleable Condensers and Their Applications,” by Xin Li of the University of Washington
− “How to Fake Auxiliary Input,” by Krzysztof Pietrzak of IST Austria
− “Information Locking from Asymptotic Geometry,” by Patrick Hayden of McGill University
− “Semantic Security in the Physical Layer,” by Alexander Vardy of the University of California, San Diego

I am grateful to the many people who contributed to the success of ICITS 2012. Above all, I thank the authors who submitted papers. ICITS exists to disseminate their research. I also thank the extremely hard-working committee members, who devoted many hours of their time and enthusiastically engaged with the new format, and the external reviewers who assisted the committee. Jürg Wullschleger deserves special thanks since he served both as a committee member and as the General Chair. His advice and help with the format and program were invaluable.

The two-track format came about after discussions with a wide range of people, including the members of the Program Committee and the ICITS Steering Committee, chaired by Yvo Desmedt. Their suggestions deserve the credit for the success of the two-track format (though I deserve the blame for any deficiencies in its implementation). I would particularly like to thank Christian Schaffner and Stephanie Wehner for a conversation at QIP during which the two-track idea was conceived (exactly nine months before ICITS!). The Steering Committee also provided useful general advice on my role as Program Committee chair. I am especially grateful to Rei Safavi-Naini, the ICITS 2008 Program Chair, for several helpful conversations.

Finally, I would like to thank Alfred Hofmann, Christine Reiss and Anna Kramer and the rest of the LNCS staff at Springer for their help preparing the proceedings.

June 2012

Program Chair

ICITS 2012
ICITS 2012

The 6th International Conference on
Information-theoretic Security
Montréal, Québec, Canada, August 15–17, 2012

Organized in cooperation with the
International Association for Cryptologic Research

General Chair
Jürg Wullschleger (Université de Montréal)

Local Co-chairs
Alain Tapp (Université de Montréal)
Claude Crépeau (McGill University)

Program Chair
Adam Smith (Pennsylvania State University)

Program Committee
Anne Broadbent University of Waterloo, Canada
Thomas Holenstein ETH Zürich, Switzerland
Yuval Ishai Technion – Israel Institute of Technology, Israel
Sidarth Jaggi Chinese University of Hong Kong, SAR China
Bhavana Kanukurthi University of California, Los Angeles, USA
Ashish Khisti University of Toronto, Canada
Yingbin Liang Syracuse University, USA
Prakash Narayan University of Maryland, USA
Louis Salvail Université de Montréal, Canada
Anand Sarwate Toyota Technological Institute at Chicago, USA
Christian Schaffner University of Amsterdam, The Netherlands
Stephanie Wehner National University of Singapore, Singapore
Daniel Wichs IBM Research, USA
Jürg Wullschleger Université de Montréal, Canada

ICITS Steering Committee
Carlo Blundo University of Salerno, Italy
Ronald Cramer CWI & 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 & Columbia University, USA
Yulian Zheng University of North Carolina, USA
External Reviewers

Prabhanjan Ananth  Eiichiro Fujisaki
Mattias Andersson  Benjamin Fuller
Gilad Asharov      Esther Hänggi
Raef Bassily       Ariel Gabizon
Amos Beimel        Adriana Lopez-Alt
Mario Berta        Samuel Ranellucci
Andrej Bogdanov    Florian Speelman
Niek Bouman        Marco Tomamichel
David Cash         Dominique Unruh
Rafael Dowsley     Mark Wilde
Serge Fehr         Stefan Wolf

Sponsors

Centre de recherches mathématiques, Université de Montréal
Institute for Quantum Computing, University of Waterloo
Institute for Transdisciplinary Research In Quantum computing (INTRIQ), a strategic cluster of the Fonds de recherche du Québec – Nature et technologies
The following papers, accepted to the “workshop track,” were presented at ICITS 2012 but do not appear as long papers in these proceedings. Authors could opt to include a one-page abstract. Abstracts of the papers marked with an asterisk appear at the end of the proceedings.

(In contrast, submissions accepted to the conference track appear as long papers. They are listed in the table of contents.)

   *Normand Beaudry, Marco Lucamarini, Stefano Mancini, Renato Renner.*

2. Share Conversion and Private Information Retrieval*
   *Amos Beimel, Yuval Ishai, Eyal Kushilevitz, Ilan Orlov*

3. Quantum to Classical Randomness Extractors
   *Mario Berta, Omar Fawzi and Stephanie Wehner*

4. Almost-Everywhere Secure Computation with Edge Corruptions*
   *Nishanth Chandran, Juan Garay, Rafail Ostrovsky*

5. Improving the Quality of Santha-Vazirani Sources*
   *Roger Colbeck and Renato Renner*

6. David and Goliath Oblivious Affine Function Evaluation*
   *Nico Döttling, Daniel Kraschewski, Jörn Müller-Quade.*

7. A Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy*
   *Benjamin Fuller, Adam O’Neill, Leonid Reyzin*

8. Feasibility and Completeness of Cryptographic Tasks in the Quantum World
   *Jonathan Katz, Fang Song, Hong-Sheng Zhou, Vassilis Zikas*

9. Bounds for Secure Two-Party Sampling from a Generalization of Common Information*
   *Vinod M. Prabhakaran, Manoj M. Prabhakaran*

10. An Information-Theoretic Approach to Privacy*
    * Lalitha Sankar, S. Raj Rajagopalan, H. Vincent Poor*

11. Polar Codes for Private Classical Communication
    *Mark Wilde, Joseph M. Renes*
# Table of Contents

Guessing Secrecy ................................................................. 1  
*Mohsen Alimomeni and Reihaneh Safavi-Naini*

Trading Robustness for Correctness and Privacy in Certain Multiparty 
Computations, beyond an Honest Majority ............................... 14  
*Anne Broadbent, Stacey Jeffery, Samuel Ranellucci, and Alain Tapp*

Two Protocols for Delegation of Computation .......................... 37  
*Ran Canetti, Ben Riva, and Guy N. Rothblum*

On the Amortized Complexity of Zero Knowledge Protocols 
for Multiplicative Relations .................................................. 62  
*Ronald Cramer, Ivan Damgård, and Valerio Pastro*

Universally Composable Oblivious Transfer from Lossy Encryption and 
the McEliece Assumptions ..................................................... 80  
*Bernardo Machado David, Anderson C.A. Nascimento, and 
Jörn Müller-Quade*

Shannon Impossibility, Revisited ............................................ 100  
*Yevgeniy Dodis*

Statistically Secure Linear-Rate Dimension Extension for Oblivious 
Affine Function Evaluation .................................................. 111  
*Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade*

Passive Corruption in Statistical Multi-Party Computation 
(Extended Abstract) ............................................................. 129  
*Martin Hirt, Christoph Lucas, Ueli Maurer, and Dominik Raub*

Efficient Threshold Zero-Knowledge with Applications to User-Centric 
Protocols .............................................................................. 147  
*Marcel Keller, Gert Læsøe Mikkelsen, and Andy Rupp*

Information-Theoretic Timed-Release Security: Key-Agreement, 
Encryption, and Authentication Codes ...................................... 167  
*Yohei Watanabe, Takenobu Seito, and Junji Shikata*

Optimum General Threshold Secret Sharing .............................. 187  
*Maki Yoshida, Toru Fujiwara, and Marc Fossorier*

**Workshop Track Abstracts** .................................................. 205

**Author Index** ..................................................................... 219