8th International Conference on Information-Theoretic Security (ICITS)

May 2-5, 2015, USI Lugano, Switzerland
www.icits2015.net

Call for Papers

This is the eighth in a series of conferences that aims to bring together the leading researchers in the areas of information theory, quantum information theory, and cryptography. ICITS covers all aspects of information-theoretic security, from relevant mathematical tools to theoretical modeling to implementation. Papers on all technical aspects of these topics are solicited for submission. Areas of interest include, but are not restricted to:

- Physical layer security
- Multiparty computation
- Codes, lattices, & cryptography
- Authentication codes
- Randomness extraction
- Cryptography from noisy channels
- Wiretap channels
- Bounded-storage models
- Information-theoretic reductions
- Quantum cryptography
- Quantum information theory
- Nonlocality and nonsignaling
- Key and message rates
- Secret sharing
- Physical models & assumptions
- Network coding security
- Adversarial channel models
- Information-theoretic tools in computational settings
- Implementation challenges
- Biometric security

Important Dates

Conference Track Submission Deadline:
November 21, 2014 (23:59 UTC)

Workshop Track Submission Deadline:
December 5, 2014 (23:59 UTC)

Notification of Decision:
January 30, 2015

Conference:
May 2-5, 2015

Note: ICITS 2015 takes place right after EUROCRYPT 2015 (April 26-30, Sofia).

Two Tracks: Conference and Workshop

As the goal of ICITS is to bring together researchers on all aspects of information-theoretic security, it consists of two tracks with different types of contributed presentations: The *conference track* which acts as a traditional conference (original papers with published proceedings) and the *workshop track* which operates more like an informal workshop, with papers that have appeared elsewhere or that consist of work in progress.

Conference Track (with proceedings) Submissions to this track must be original papers that have not previously appeared in published form. Accepted papers will be presented at the conference and will also be published in

the conference proceedings (which will appear in Springer's Lecture Notes in Computer Science series). We note that simultaneous submission to journals is acceptable, but simultaneous submission to other conferences with published proceedings is not.

Workshop Track (no proceedings) To encourage presentation of work from a variety of fields (especially those where conference publication is unusual or makes journal publication difficult), the committee also solicits "workshop track" papers. Accepted papers will be presented orally at the conference but will not appear in the proceedings. Submissions to this track that have previously appeared (or are currently submitted elsewhere) are acceptable, as long as they first appeared after January 1, 2014. Papers that describe work in progress are also welcome. We note that the same standards of quality will apply to conference and workshop papers.

Instructions for Authors

Conference Track: Submissions must not substantially duplicate work published elsewhere or submitted in parallel to a journal or any other conference/workshop that has proceedings. The submission must be **anonymous**, with no author names, affiliations, or obvious references. The length of the submission must be at most 12 pages excluding bibliography and appendices. The text must be in a single column format, use at least 11-point fonts, and have reasonable margins. The submission should begin with a title and a short abstract. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them. Submissions should preferably be in PDF format. Instructions on how to submit will be provided on the web site.

Workshop Track: Authors may submit a paper published elsewhere or an original manuscript. As with the conference track, submissions should begin with a title and short abstract followed by an introduction that summarizes the contributions at a level appropriate for a non-specialist reader. Information about previous publication, if any, should be indicated on the first page of the submission. Beyond these guidelines no specific format is required. In particular, (a) papers previously published elsewhere may be submitted in their published form provided bibliographic information is clearly indicated; (b) short summaries of works available in other venues or online (on the arXiv or IACR eprint) are acceptable; (c) original submissions may be left anonymous at the discretion of the authors. (Previously published submissions cannot be anonymous.)

There is no restriction on program committee member submissions to either track, though PC-authored papers will be held to a higher standard.

Conference Organization

General and Program Co-Chairs:

Anja Lehmann *(IBM Research Zurich, Switzerland)*
Stefan Wolf *(USI Lugano, Switzerland)*

Program Committee

Paolo D'Arco *(University of Salerno, Italy)*
Paulo Barreto *(University of São Paulo, Brazil)*
Mario Berta *(Caltech, USA)*
Anne Broadbent *(University of Ottawa, Canada)*
Roger Colbeck *(University of York, UK)*
Frédéric Dupuis *(Århus University, Denmark)*
Stefan Dziembowski *(University of Warsaw, Poland)*
Sebastian Faust *(EPF Lausanne, Switzerland)*
Omar Fawzi *(ETH Zurich, Switzerland)*
Peter Gazi *(IST, Austria)*
Yuval Ishai *(Technion, Israel)*
Anja Lehmann *(IBM Research Zurich, Switzerland)*
Keith Martin *(Royal Holloway, University of London, UK)*
Prakash Narayan *(University of Maryland, USA)*
Anderson Nascimento *(University of Brasilia, Brazil)*
Koji Nuida *(AIST, Japan)*
Frederique Oggier *(Caltech, USA)*
Claudio Orlandi *(Århus University, Denmark)*
Carles Padro *(Polytechnic University of Catalonia, Spain)*
Rei Safavi-Naini *(University of Calgary, Canada)*
Marco Tomamichel *(University of Sidney, Australia)*
Stefan Wolf *(USI Lugano, Switzerland)*
Mark Zhandry *(Stanford University, USA)*