ICITS 2012

6th International Conference on Information-Theoretic Security

Montréal, Québec, Canada
August 15–17, 2012
`http://icits2012.iro.umontreal.ca/`

Call for Papers

This is the sixth 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 computations	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
Implementation challenges	Biometric security	in computational settings

Important Dates

Conference Track Submissions due	~~Monday, March 12~~ **Thursday, March 22, 2012, 3pm EDT**
Conference Track Notification	Friday, May 4, 2012
Proceedings version due	Tuesday, May 29, 2012
Workshop Track Submissions due	**Monday, April 9, 2012, 3:00 pm EDT**
Workshop Track Notification	Monday, May 28, 2012

ICITS (Aug. 15–17, Montreal) is the week before CRYPTO 2012 (Aug. 20–23, Santa Barbara).

Two Tracks: Conference and Workshop

The goal of ICITS is to bring together researchers on all aspects of information-theoretic security. To this end, ICITS 2012 will consist of two types of contributed presentations. The conference track will act as a traditional conference (original papers with published proceedings). The workshop track will operate 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, 2011. Papers that describe work in progress are also welcome. We note that the same standards of quality will apply to conference and workshop papers.

It is not possible to submit the same work for consideration in both tracks.

Conference Organization

General Chair	Jürg Wullschleger *(Université de Montréal)*
Local Co-Chairs	Claude Crépeau *(McGill University)*
	Alain Tapp *(Université de Montréal)*
Program Chair	Adam Smith *(Pennsylvania State University)*

Program Committee

Anne Broadbent *(University of Waterloo)*
Yuval Ishai *(Technion)*
Bhavana Kanukurthi *(UCLA)*
Yingbin Liang *(Syracuse University)*
Louis Salvail *(Université de Montréal)*
Christian Schaffner *(University of Amsterdam)*
Stephanie Wehner *(National U. Singapore)*
Jürg Wullschleger *(Université de Montréal)*
Thomas Holenstein *(ETH Zürich)*
Sidharth Jaggi *(Chinese U. of Hong Kong)*
Ashish Khisti *(University of Toronto)*
Prakash Narayan *(University of Maryland)*
Anand Sarwate *(TTI Chicago)*
Adam Smith *(Pennsylvania State University)*
Daniel Wichs *(IBM Research)*

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. A link to the submission site can be found 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.