The 4th International Conference on Information Theoretic Security - ICITS 2009

December 3-6, 2009, Shizuoka, JAPAN

Note: Asiacrypt will be held in December 6-10 in Tokyo, JAPAN

Call for Papers

Over the last few decades, we have seen several research topics studied requiring information theoretical security, also called unconditional security, where there is no unproven computational assumption on the adversary. (This is the framework proposed by Claude Shannon in his seminal paper.) Also, coding as well as other aspects of information theory have been used in the design of cryptographic schemes. Examples are authentication, secure communication, key exchange, multi-party computation and information hiding to name a few. A related area is quantum cryptography that predominantly uses information theory for modeling and evaluation of security. Needless to say, information theoretically secure cryptosystems are secure even if the factoring assumption or the discrete log assumption are broken. Seeing the multitude of topics in modern cryptography requiring information theoretical security or using information theory, it is time to have a regular conference on this topic.

This is the 4th conference of this series that is aimed to bring together the leading researchers in the area of information and/or quantum theoretic security. Original research papers on all technical aspects of information and/or quantum theoretic security are solicited for submission to ICITS 2009.

The topics of interest are (but not limited to):

Information Theoretic Analysis of Security
Public Key Cryptosystems using Codes
Conventional Cryptography using Codes
Authentication Codes
Key Distribution
Quantum Cryptography
Quantum Information Theory
Randomness Extraction
Secret Sharing
Secure Multiparty Computation
Oblivious Transfer
Anonymity
Ideal Ciphers
Traitor Tracing
Fingerprinting
Data Hiding and Watermarking
Information Hiding
Private and Reliable Networks

History:

The 1st ICITS was held in October 16-19, 2005 in Japan under the name of 2005 IEEE Information Theory Workshop on Theory and Practice (ITW 2005), where the general co-chairs were Hideki Imai and Yuliang Zheng, and the program chair was Ueli Maurer. The 2nd ICITS was held in Madrid after Eurocrypt 2007, where the program chair was Yvo Desmedt. The 3rd ICITS was held in Calgary before CRYPTO 2008, where the program chair was Rei Safavi-Naini. These three conferences were great success.

Important dates are:

Submission deadline	Decision notification	Pre-proceedings version	Proceedings version
August 13, 2009	~~September 15, 2009~~ September 28, 2009	October 12, 2009	December 23, 2009

Instructions for Authors:

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has 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.
- We strongly encourage to use Springer's LNCS format for submissions. The final proceedings version will be a paper of at most 18 pages in the llncs style, which corresponds to around 7000 words of text. The document submitted (excluding appendices) should correspond to what the author expects to be published if their paper is accepted without modification. We therefore strongly recommend that authors check whether their paper (without appendices) will fit within the above llncs space constraints.
- The submission should begin with a title, a short abstract, and a list of keywords. 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 (pdf file) although PostScript (ps file) will be allowed.
- Please submit your papers via the following link .
  https://secure.iacr.org/websubrev/icits2009/submit/index.php
- Submission deadline : Thu, 13 Aug 2009 12:00:00 +0000 (UTC)

Proceedings: Proceedings will be published from Springer's *Lecture Notes in Computer Science*.
(Pre-proceedings will be given at the conference.)

General Chair: Akira Otsuka
National Institute of Advanced Industrial Science and Technology, Japan
and Chuo University, Japan
Email: icits2009@m.aist.go.jp

Program Chair: Kaoru Kurosawa
Ibaraki University, Japan
Email: ICITS2009@mx.ibaraki.ac.jp

Local Organizer: Yukiko Ito
National Institute of Advanced Industrial Science and Technology, Japan
Email: icits2009@m.aist.go.jp

Advisor: Hideki Imai
National Institute of Advanced Industrial Science and Technology, Japan
and Chuo University, Japan
Email: icits2009@m.aist.go.jp

Program Committee

Carlo Blundo (University of Salerno, Italy)
Paolo D'Arco (University of Salerno, Italy)
Stefan Dziembowski (Universitá La Sapienza, Italy)
Serge Fehr (CWI, The Netherlands)
Juan Garay (AT&T Labs-Research, USA)
Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology, Japan)
Kaoru Kurosawa (Ibaraki University, Japan) Chair
Hoi-Kwong Lo (University of Toronto, Canada)
Keith Martin (Royal Holloway, University of London, UK)
Ueli Maurer (ETH, Switzerland)
Jesper Buus Nielsen (University of Aarhus)
Renato Renner (ETH, Switzerland)
Rei Safavi-Naini (University of Calgary, Canada)
Thomas Shrimpton (University of Lugano, Switzerland)
Doug Stinson (University of Waterloo, Canada)
Stefan Wolf (ETH, Switzerland)
Moti Yung (RSA & Columbia University, USA)
Yuliang Zheng (University of North Carolina, USA)

Steering Committee

Carlo Blundo (University of Salerno, Italy)
Gilles Brassard (University of Montreal, Canada)
Ronald Cramer (CWI, The Netherlands)
Yvo Desmedt, Chair (University College London, UK)
Hideki Imai (National Institute of Advanced Industrial Science and Technology, Japan)
Kaoru Kurosawa (Ibaraki University, Japan)
Ueli Maurer (ETH, Switzerland)
C. Pandu Rangan (IIT, Chennai, India)
Rei Safavi-Naini (University of Calgary, Canada)
Doug Stinson (University of Waterloo, Canada)
Moti Yung (RSA & Columbia University, USA)
Yuliang Zheng (University of North Carolina, USA)