The 2nd International Conference on Information Theoretic Security (ICITS)

Calgary, Canada, August 10-13, 2008

Call for Papers

Submission Deadline : March 23rd, 2008

Note: Crypto Conference is held August 17-21, 2008 in Santa Barbara, USA.

Scientific study of cryptography started with the seminal paper of Shannon on secrecy systems. Since then, information theoretic approach has been used to model a range of other security properties and evaluate performance of systems. This includes key agreement, multiparty computation, secret sharing and private information retrieval to name a few. A related area of security is quantum cryptography that predominantly uses information theory for modeling and evaluation of security. More recently quantum theoretic assumptions have been successfully used to enhance classical models. Information theoretic security provides security without any computational assumption and will be of increasing importance when long term security must be guaranteed..

This is the second conference in a series of conferences that is aimed to bring together the leading researchers in the area of information and quantum theoretic security.

Background: This series of conferences is a successor to the 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005, Japan http://imailab-www.iis.u-tokyo.ac.jp/~itw05/) October 16-19, 2005. The first ICITS conference was held in Madrid http://www.escet.urjc.es/~matemati/maribel/ICITS/ITS07.htm, after Eurocrypt 2007.

Proceedings: Conference proceedings will be published by Springer in the Lecture Notes in Computer Science series.

Topics of interest: The topics of interest are all aspects of information theoretic security that includes, but is not limited to the following topics:

- Information theoretic analysis of security
- Anonymity
- Private and Reliable Networks
- Public Key Cryptosystems using Codes

- Authentication Codes
- Conventional Cryptography using Codes
- Fingerprinting
- Ideal Ciphers
- Information Hiding
- Key Distribution
- Oblivious Transfer
- Quantum Cryptography
- Quantum Information Theory
- Randomness extraction
- Secret Sharing
- Secure Multiparty Computation
- Non-standard models
- Data hiding and Watermarking

Notes: The focus of the conference is information theoretic security and so papers on construction of codes and sequences need clear justification and evaluation of security applications.

Venue: Calgary is a city of one million inhabitants in the foothills of the magnificent Canadian Rocky Mountains. In addition to planned excursions, Calgary is close to Banff National Park and offers many summertime recreational activities including hiking, whitewater rafting and kayaking, climbing, caving, mountain-lake scuba diving, mountain biking, glacier trips, hang gliding, and horseback riding. August is an excellent month for recreation due to its clement warm and usually dry weather.

Instructions for Authors: The paper must start with a title, an abstract and keywords, but should be **anonymous**. It should be followed by a succinct statement appropriate for a non-specialist reader specifying the subject addressed, its background, the main achievements, and their significance to information theoretic security. Technical details directed to the specialist should then follow. Self citations to unpublished work should be avoided to maintain the anonymity. A limit of 12 single spaced pages of 11pt type (not counting the bibliography and clearly marked appendices) is placed on all submissions. The total paper must not exceed 20 pages. Since referees are not required to read the appendices, the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits.

Submission instructions: Abstracts that have been or will be submitted in parallel to other conferences and workshops that have proceedings are **not** eligible for submission. One of the authors is expected to present the paper.

The submission receipt deadline is March 23, 2008. Instructions on how to submit electronically will be posted soon on http://iqis.org/events/icits2008/

Important dates:

Submission Deadline:	March 23, 2008
Notification:	May 11, 2008

Proceedings versions due: June 1, 2008

Program Committee:

Simon Blackurn	Royal Holloway University of London, UK
Carlo Blundo	University of Salerno, Italy
Stefan Dziembowski	Università La Sapienza, Italy
Cunsheng Ding	Hong Kong University of Science and Technology, HK
Yevgeniy Dodis	New York University, USA
Paolo D’Arco	University of Salerno, Italy
Serge Fehr	CWI, The Netherland
Matthias Fitzi	Århus University, Denmark
Hideki Imai	Chuo University, Japan
Kaoru Kurosawa	Ibaraki University, Japan
Jorn Muller-Quade	Universität Karlsruhe, Germany
Dingyi Pei	Academia Sinica, People Republic of China
C. Pandu Rangan	Indian Institute of Technology, India
Renato Rennner	ETH, Switzerland
Rei Safavi-Naini (Chair)	University of Calgary, Canada
Alain Tapp	Universite d’ Montreal, Canada
Huaxiong Wang	Nanyang Technological University, Singapore
Wolfgang Tittel	University of Calgary, Canada
Moti Yung	Columbia University, USA
Yuliang Zheng	University of North Carolina, USA

General Chair:
Barry Sanders

Steering Committee:

Carlo Blundo (Univ. of Salerno, Italy)

Gilles Brassard (Univ. of Montreal, Canada)

Ronald Cramer (CWI, The Netherlands)

Yvo Desmedt, (Univ. College London, UK)

Hideki Imai (National Inst.of Adv. Industrial Sci. and Tech., Japan)

Kaoru Kurosawa (Ibaraki Univ, Japan)

Ueli Maurer (ETH, Switzerland)

C. Pandu Rangan (IIT, Chennai, India)

Rei Safavi-Naini (Univ of Calgary, Canada)

Doug Stinson (Univ of Waterloo, Canada)

Moti Yung (Columbia University, USA)

Yuliang Zheng (Univof North Carolina, USA)