International Conference on Information Theoretic Security (ICITS)

Madrid, Spain, May 25-29, 2007

Call for Papers

Extended Submission Deadline: March 9, 2007

Note: Eurocrypt is May 20-24, 2007 in Barcelona, Spain.

Background For the last years we have plenty of conferences and workshops on specialized topics in cryptography. Examples are CHES, FSE, PKC and TCC. The modern unclassified research on cryptography started with Shannon's work on cryptography using information theory. Since then we have seen several research topics studied requiring information theoretical security, also called unconditional security. Examples are anonymity, authenticity, reliable and private networks, secure multi-party computation, traitor tracing, etc. Moreover, we have also seen that coding as well as other aspects of information theory have been used in the design of cryptographic schemes.

Seeing the multitude of topics in cryptography requiring information theoretical security or using information theory, it is time to have a regular conference on this topic. This was first realized by Prof. Imai (University of Tokyo, Japan). He organized the 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005, Japan) October 16-19, 2005. The goal is to continue this event on a regular basis. However, while ITW 2005 was organized by IEEE, this one will not. The main reason is that it is the goal to have the proceedings published by Springer in the Lecture Notes in Computer Science.

Proceedings Post-conference proceedings will be published by Springer Verlag in the Lecture Notes in Computer Science. Informal preproceedings will be available at the conference.

Topics of interest The topics of interest are on work on any aspect of information theoretical security, this means *security based on information theory*. This includes, but is not limited to the following topics:

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

Notes: papers on coding theory without any relationship with cryptography will be rejected. It is *not* the goal of this conference to become a second one on "Coding and Cryptography." Papers using computational complexity assumptions, except when using: information theoretic results or quantum arguments, will not be accepted.

Venue Madrid is a city with a long history and very good airport connections. Its climate end of May is pleasantly warm. Madrid has good connections to the rest of the world and the rest of Spain, in particular Barcelona. More information on how to reach the venue by airplane or train will be provided later. Madrid is very close to Toledo, a small historical city worth visiting.

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 singlespaced 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 or 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 9, 2007. Instructions on how to submit electronically are posted on: ICITS

Important dates

Submission Deadline:	March 9, 2007
Authors Informed:	April 23, 2007
Preproceedings versions due:	May 7, 2007

Program 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)
Matthias Fitzi (Århus University, Denmark)
Hideki Imai (National Institute of Advanced Industrial Science and Technology, Japan)
Kaoru Kurosawa (Ibaraki University, Japan)
Keith Martin (Royal Holloway, UK)
Rei Safavi-Naini (University of Wollongong, Australia)
Doug Stinson (University of Waterloo, Canada)
Stefan Wolf (ETH, Switzerland)
Moti Yung (RSA & Columbia University, USA)
Yuliang Zheng (University of North Carolina, USA)

Submission receipt deadline: March 9, 2007

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)
Rei Safavi-Naini (University of Wollongong, Australia)
Doug Stinson (University of Waterloo, Canada)
Moti Yung (RSA & Columbia University, USA)
Yuliang Zheng (University of North Carolina, USA)

General and Local Chairs

General Chair:	Javier Lopez
Local Co-Chairs:	Julio Cesar Hernandez, and Maria Isabel Gonzalez Vasco