

Thirteenth IMA International Conference on **CRYPTOGRAPHY AND CODING**

12th - 15th December 2011, Lady Margaret Hall, University of Oxford, UK

CALL FOR PAPERS

The mathematical theory and practice of cryptography and coding underpins the provision of effective security and reliability for data communication, processing and storage. Theoretical and practical advances in the fields of cryptography and coding are therefore a key factor in facilitating the growth of data communications and data networks of various types. Thus, this thirteenth International Conference in an established and successful IMA series on the theme of "Cryptography and Coding" is both timely and relevant.

This event has been running since 1986, and this year is the 25th anniversary of the conference! We are going to have a joint 25 anniversary celebration with Cryptomathic. We have four distinguished keynote speakers: Professor Ivan Damgård, Professor Paddy Farrell, Professor Jonathan Jedwab and Professor David Naccache.

Original research papers on all technical aspects of cryptography and coding are solicited for submission. The proceedings will be published in the Springer Lecture Notes in Computer Science series, and will be available at the conference.

Important Dates:

Submission deadline (extended): June 24, 2011

Notification of decision: August 29, 2011

Proceedings version deadline: September 17, 2011

Conference: December 12-15, 2011

Instructions for Authors:

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. Submitted papers must be in PDF format and should be submitted electronically to the submission server at

<https://www.easychair.org/conferences/?conf=imacc2011>

All submissions will be blind-reviewed. Papers must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. A submitted paper should begin with a title, a short abstract, and a list of keywords. The length of submissions must be at most 15 pages excluding references and appendices. Committee members are not required to review appendices, so the paper should be intelligible and self-contained within this length. The text should be in a single column format, in at least 11-point fonts and have reasonable margins. Submissions not meeting these guidelines risk rejection without consideration of their merits.

It is strongly recommended that submissions be processed using LaTeX2e according to the instructions listed on Springer's web site. These instructions are mandatory for the final papers. If a submission is accepted, the length of the final version for Springer's LNCS will be at most 20 pages including references and appendices. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Programme Committee:

Dr. Liqun Chen (Hewlett-Packard Laboratories) (Programme Chair)
Dr. Steve Babbage C.Math. FIMA (Vodafone)
Dr. Mohammed Benaissa (University of Sheffield)
Prof. Nigel Boston (Wisconsin)
Prof. Colin Boyd (Queensland University of Technology)
Prof. Pascale Charpin (INRIA Rocquencourt)
Dr. Carlos Cid (Royal Holloway, University of London)
Dr. Nicolas T. Courtois (University College London)
Prof. James Davenport (University of Bath)
Prof. Tuvi Etzion (Technion)
Prof. Dieter Gollmann (TUHH)
Mr. Keith Harrison (Hewlett-Packard Laboratories)
Prof. David Jao (University of Waterloo)
Prof. Jon-Lark Kim (University of Louisville)
Prof. Mirosław Kutylowski (Wrocław University of Technology)
Dr. Gohar Kyureghyan (University of Magdeburg)
Prof. Xuejia Lai (Shanghai Jiao Tong University)
Prof. Pil Joong Lee (Pohang University of Science & Technology)
Prof. Dongdai Lin (Institute of Software Chinese Academy of Sciences)
Dr. Catherine Meadows (Naval Research Laboratory)
Prof. Gary McGuire (University College Dublin)
Prof. David Naccache (Ecole Normale Supérieure)
Dr. Siaw-Lynn Ng (Royal Holloway, University of London)
Prof. Matthew G. Parker (University of Bergen)
Dr. Raphael Phan (Loughborough University)
Dr. Matt Robshaw (France Telecom)
Dr. Ana Salagean (Loughborough University)
Dr. Hans Georg Schaathun (Ålesund University College)
Prof. Michael Scott (Dublin City University)
Dr. Martijn Stam (University of Bristol)
Dr. Frederik Vercauteren (K. U. Leuven)
Dr. Guilin Wang (University of Wollongong)
Dr. Bogdan Warinschi (University of Bristol)
Prof. Kyeongcheol Yang (Pohang University of Science and Technology)
Dr. Jianying Zhou (I2R)

Steering Committee:

Prof. Steven Galbraith (University of Auckland)
Prof. Bahram Honary C.Math. FIMA (Lancaster University)
Prof. Chris Mitchell C.Math. FIMA (Royal Holloway, University of London)
Prof. Matthew G. Parker (University of Bergen)
Prof. Kenny Paterson FIMA (Royal Holloway, University of London)
Prof. Fred Piper C.Math. FIMA (Royal Holloway, University of London)
Prof. Nigel Smart (University of Bristol)
Prof. Mike Walker C.Math. FIMA (Vodafone and Royal Holloway)

Sponsors:

Cryptomathic
Hewlett-Packard
Vodafone

For more information about the conference, please see the conference web site: http://www.hpl.hp.com/personal/Liqun_Chen/IMACC11-home.htm

