INTERNATIONAL WORKSHOP ON CODING AND CRYPTOGRAPHY

WCC 2005

March 14–18, 2005, Bergen, Norway

ANNOUNCEMENT AND CALL FOR PAPERS

The workshop is organized by Selmersenteret and IN-RIA, and sponsored by the Norwegian Research Council. It will take place in the center of Bergen.

Conference Themes: Our aim is to bring together researchers in all aspects of coding theory, cryptography and related areas, theoretical or applied.

Deadlines:
- Reception of extended abstract by December 15, 2004
- Notification by January 31, 2005
- Final version for the book of abstracts by February 14, 2005

Topics include, but are not limited to:
- coding theory: error-correcting codes, decoding algorithms, related combinatorial problems;
- cryptology: block and stream ciphers, hash functions, public key cryptography, secret sharing, authentication, intellectual property protection...
- Discrete mathematics and algorithmic tools arising from these two areas, such as: Boolean functions, sequences, finite fields, algebraic systems and related polynomial properties...

Those wishing to contribute a 20 minute talk are invited to submit a 6-10 page extended abstract, before December 15, 2004, by sending an electronic copy (LaTeX or Postscript, see instructions to authors on the web site). If electronic submission is impossible, you may submit instead three hard copies to

Pascale Charpin, Program committee of WCC 2005, INRIA, Projet CODES
BP 105, 78153 Le Chesnay Cedex, France

A volume including the accepted abstracts will be provided to the participants.

Full papers : All authors of accepted abstracts will be invited to submit a full paper for the proceedings to appear as a special issue of Discrete Applied Mathematics journal. Every contribution will be thoroughly refereed.

Local Organizing Committee: T. Helleseth (**chair**); Selmersenteret

Program committee: D. Augot (**submissions**, INRIA Rocquencourt, France), C. Carlet (Université Paris VIII, France), P. Charpin (**co-Chair**, INRIA Rocquencourt, France), C. Ding (Hong Kong University of Science and Technology, China), H. Dobbertin (University of Bochum, Germany), S. Dodunekov (Institute of Mathematics, Sofia, Bulgaria), I. Dumer (UC Riverside),G. Gong (University of Waterloo, Canada), T. Helleseth (University of Bergen, Norway), I. Honkala (University of Turku, Finland), T. Høholdt (DTU, Denmark), T. Johansson (Lund University, Sweden), G. Kabatianski (IPIT, Moscow, Russia), T. Lange (University of Bochum, Germany), J. Massey (Lund University, Sweden), M. Mihaljevic (Serbian Acad. Of Sciences and Art, Serbia and Montenegro), K. Nyberg (Nokia, Finland), M. G. Parker (University of Bergen, Norway), K. Paterson (Royal Holloway, England), I. Semaev (University of Bergen, Norway), N. Sendrier (INRIA, France), D. Stinson (University of Waterloo, Canada), H. van Tilborg (Eindhoven University of Technology, The Netherlands), S. Vladuts (Université de Marseille, France), Ø. Ytrehus (**co-Chair**, University of Bergen, Norway), G. Zémor (ENST, France), V. Zinoviev (IPIT, Moscow, Russia)

Invited talks:
- A. Canteaut (INRIA)
- R. Koetter (University of Illinois, Urbana-Champaign)
- P. V. Kumar (University of Southern California)
- T. Kalker (Hewlett-Packard Labs)

Information: http://www.selmer.uib.no/WCC.html or e-mail to wcc@ii.uib.no