

JOURNÉES INTERNATIONALES
CODAGE ET CRYPTOGRAPHIE
WCC 2003

24-28 Mars 2003, Versailles, France

ANNONCE ET APPEL À COMMUNICATION



Les journées sont organisées par l'INRIA et par l'ENSTA avec le soutien de l'Ecole Supérieure et d'Application des Transmissions. Elles auront lieu à l'INRIA près de Versailles à 20 km de Paris.

► **Objectifs de la conférence :**

Notre but est de rassembler les chercheurs dans tous les aspects de la théorie des codes, de la cryptologie et des domaines associés, théoriques ou appliqués.

► **Dates limites :**

- Soumission des résumés : le 29 novembre 2002.
- Notification : le 31 janvier 2003.
- Version finale pour le livre des résumés : le 14 février 2003.

► **Les thèmes seront, en particulier :**

- théorie des codes : codes correcteurs d'erreurs, algorithmes de décodage, problèmes de combinatoire associés ;
- cryptologie : chiffrement par bloc et à flot, fonctions de hachage, cryptographie à clé publique, partage du secret, authentification, protection des droits d'auteurs ;
- outils d'algorithmique et de mathématiques discrètes issus de ces deux disciplines tels que : les fonctions booléennes, les séquences, les corps finis, les systèmes algébriques et les propriétés de polynômes associées.

Les personnes désireuses de proposer une contribution, sous la forme d'un exposé d'une vingtaine de minutes, sont invitées à soumettre un résumé long de 6 à 10 pages, avant le 29 novembre 2002, sous forme électronique (Postscript ou PDF, voir les instructions aux auteurs sur la page web). Si la soumission électronique est impossible, trois exemplaires papier pourront être envoyés à

Pascale Charpin, Comité de programme de WCC 2003,
INRIA, Projet CODES
BP 105, 78153 Le Chesnay Cedex, France

Un livre contenant le résumé de chaque exposé accepté sera publié et remis aux participants.

► **Articles complets :**

Les auteurs des résumés acceptés seront invités à soumettre un papier long pour les actes de la conférence qui paraîtront en tant que numéro spécial de la revue « Discrete Applied Mathematics ». Les contributions retenues seront rigoureusement sélectionnées.



► **Comité d'organisation :**

A. Canteaut (INRIA, France), E. Filiol (ESAT, France), C. Fontaine (Université de Lille, France), P. Gaborit (Université de Limoges, France), F. Levy-dit-Vehel (ENSTA, France), P. Loidreau (**Président**, ENSTA, France), N. Sendrier (INRIA, France), J.-P. Tillich (INRIA, France).

► **Organisation locale :**

D. Potherat (INRIA, France).

► **Comité de programme :**

D. Augot (**soumissions**, INRIA, France),
C. Bachoc (Université de Bordeaux, France),
A. Barg (Bell Laboratories, USA),
T. Berger (Université de Limoges, France),
C. Carlet (Université Paris VIII, France),
P. Charpin (**co-Présidente**, INRIA, France),
C. Ding (Hong Kong University of Science and Technology, Chine),
S. Dodunekov (Institute of Mathematics, Sofia, Bulgarie),
T. Ericsson (Linköping University, Suède),
P. Fitzpatrick (University of Cork, Irlande),
E. Gabidulin (MIPT, Russie),
M. Girault (France Télécom R&D, France),
G. Gong (University of Waterloo, Canada),
T. Helleseeth (University of Bergen, Norvège),
T. Høholdt (Technical University of Denmark, Danemark),
I. Honkala (University of Turku, Finlande),
R. Johannesson (Lund University, Suède),
T. Johansson (Lund University, Suède),
G. Kabatianski (**co-Président**, IPIT, Moscow, Russie),
J. Massey (Lund University, Suède),
M. Matsui (Mitsubishi Electric Corporation, Japon),
F. Morain (École Polytechnique, France),
H. Niederreiter (National University of Singapore, Singapour),
V. Pless (University of Illinois at Chicago, USA),
H. van Tilborg (Eindhoven University of Technology, Pays-Bas),
S. Vladuts (Université de Marseille, France),
V. Zinoviev (IPIT, Moscow, Russie),
G. Zémor (ENST, France).

► **Conférenciers invités :**

- H. Dobbertin, (Bochum University, Allemagne)
- I. Dumer, (University of California, USA)
- J.-C. Faugère, (Université Paris VI, INRIA, France)
- U. Maurer, (ETH Zürich, Suisse)

Informations :

<http://www-rocq.inria.fr/codes/WCC2003/>

ou par mél à

wcc-orga@inria.fr