JOURNÉES "CODAGE ET CRYPTOGRAPHIE"

11-14 janvier 1999, Paris, France

ANNONCE ET APPEL À CONTRIBUTION

Les journées sont organisées par l'INRIA avec le soutien du Centre de Recherche des Écoles de Coëtquidan, et se dérouleront à Paris du 11 au 14 janvier 1999.

Objectifs de la conférence : Notre but est de rassembler des chercheurs dans tous les domaines, théoriques et appliqués, liés au codage et à la cryptographie.

Dates limites :

- Soumission : le 2 octobre 1998
- Notification : le 13 novembre 1998
- Résumé final : le 27 novembre 1998

Les thèmes seront, en particulier :

- théorie des codes : codes en bloc (linéaires et non-linéaires), codes cycliques, codes euclidiens, rayon de recouvrement, distributions de poids, décodage à décisions souples ; codes convolutifs, codes concaténés parallèles et séries (turbo), décodage à sortie souple ;
- cryptologie : chiffrement par bloc ou à flot, fonctions de hachage, cryptographie à clé publique, signature digitale, partage du secret, authentification, cryptanalyse, protection des droits d'auteur ;
- liens entre ces deux disciplines : groupes finis, corps finis, géométrie algébrique, corps de fonctions, structures aléatoires, réseaux, combinatoire, designs, fonctions booléennes, séquences.

Les personnes désirant proposer une contribution, sous la forme d'un exposé d'une vingtaine de minutes, sont invitées à soumettre un résumé long de 2 à 10 pages, avant le 2 octobre 1998, soit en envoyant trois copies papier à

Claude Carlet, WCC 99,
INRIA, Projet CODES
BP 105, 78153 Le Chesnay Cedex, France

soit, de préférence, une copie électronique (LaTeX ou postscript) par mél à `wcc-prog@inria.fr`.
Un livre contenant le résumé de chaque exposé accepté sera publié par l'INRIA et remis aux participants.

Comité d'organisation : C. Carlet (INRIA et Université de Caen, France), G. Cohen (Président du chapitre français de IEEE-IT, France), C. Fontaine (INRIA, France), E. Filiol (Centre de Recherche des Écoles de Coëtquidan, France), S. Harari (Université de Toulon, France), N. Sendrier (**Président**, INRIA, France),

Organisation locale : A. Theis-Viemont (INRIA, France), C. Thenault (INRIA, France).

Comité de programme : D. Augot (INRIA, France), J. Boutros (ENST, France), T. Berger (Université de Limoges, France), A. Burr (University of York, UK), A. Canteaut (INRIA, France), C. Carlet (**Président**, INRIA et Université de Caen, France), P. Charpin (INRIA, France), G. Cohen (ENST, France), J.-M. Couveignes (DGA et Université de Bordeaux, France), P. Farrell (University of Manchester, UK), A. Glavieux (ENST-Bretagne, France), S. Harari (Université de Toulon, France), G. Kabatiansky (Russian Academy of Sciences, Russia), D. Lebrigand (Université Paris 6, France), S. Litsyn (University of Tel Aviv, Israel), H. Mattson (University of Syracuse, USA), F. Morain (DGA et École Polytechnique, France), N. Sendrier (INRIA, France), S. Shepherd (University of Bradford, UK), H. Van Tilborg (Eindhoven University of Technology, The Netherlands).

Conférenciers invités :

- Hans Dobbertin, Allemagne
- Ernst Gabidulin, Russie
- James Massey, Danemark
- Vera Pless, USA
- John Dillon, USA (sous réserve)

Informations: `http://www-rocq.inria.fr/codes/WCC99/` ou mèl à `wcc-orga@inria.fr`