Actes des Journées Internationales Codage et Cryptographie,
24-28 Mars 2003, Versailles (France).

Organisé par l'INRIA et l'ENSTA.
Edité par Daniel Augot, Pascale Charpin and Grigory Kabatianski.

Proceedings of the International Workshop on Coding and Cryptography, March 24-28 2003, Versailles (France).

Organized by INRIA and ENSTA.
Edited by Daniel Augot, Pascale Charpin and Grigory Kabatianski.

**Comité de Programme — Program committee**

D. Augot (submissions) INRIA Rocquencourt, France
C. Bachoc Université de Bordeaux, France
A. Barg Bell Laboratories, USA
T. Berger Université de Limoges, France
C. Carlet Université Paris 8, France
P. Charpin (co-chair) INRIA Rocquencourt, France
C. Ding Hong Kong University of Science and Technology, China
S. Dodunekov Institute of Mathematics, Sofia, Bulgaria
T. Ericsson Linköping University, Sweden
P. Fitzpatrick University of Cork, Ireland
E. Gabidulin MIPT, Russia
M. Girault France Telecom R&D, France
G. Gong University of Waterloo, Canada
T. Helleseth University of Bergen, Norway
T. Høholdt Technical University of Denmark, Denmark
I. Honkala University of Turku, Finland
R. Johannesson Lund University, Sweden
T. Johansson Lund University, Sweden
G. Kabatianski (co-chair) IPIT, Moscow, Russia
J. Massey Lund University, Sweden
M. Matsui Mitsubishi Electric Corporation, Japan
F. Morain École Polytechnique, France
H. Niederreiter National University of Singapore, Singapore
V. Pless University of Illinois at Chicago, USA
H. van Tilborg Eindhoven University of Technology, The Netherlands
S. Vladuts Université de Marseille, France
G. Zémor ENST, France
V. Zinoviev IPIT, Moscow, Russia

**Comité d'organisation — Organization committee**

A. Canteaut INRIA Rocquencourt, France
E. Filiol Ecole Supérieure et d'Application des Transmissions, France
C. Fontaine Université de Lille, France

P. Gaborit Université de Limoges, France

F. Levy-dit-Vehel Ecole Nationale Supérieure de Techniques Avancées, France

P. Loidreau Ecole Nationale Supérieure de Techniques Avancées, France (Chair)

N. Sendrier INRIA Rocquencourt, France

J.-P. Tillich INRIA Rocquencourt, France

**Organisation Locale — Local organization**

C. Girodon INRIA Rocquencourt, France

**Sponsors**

INRIA

Ecole Supérieure et d'Application des Transmissions

Université de Limoges

Délégation Générale pour l'Armement (DGA)

European Research Consortium for Informatics and Mathematics (ERCIM)

France Télécom




**Avant-propos**

Soyez tous les bienvenus à ces journées internationales sur le Codage et la Cryptographie à l'unité de recherche INRIA-ROCQUENCOURT[1]. Cet avant-propos nous permet de remercier tous les membres du comité de programme pour leur excellent travail de sélection des résumés soumis. Chacune des 107 soumissions a été évaluée par deux rapporteurs; 51 d'entre elles ont été acceptées.

Pour certaines soumissions, les membres du comité ont reçu l'aide d'autres chercheurs. Nous remercions *Ali Akhavi, François Arnault, Bram van Asch, Magali Bardet, Peter Beelen, Peter Biyvalenkov, Sebastien Canard, Anne Canteaut, Gerard Cohen, Andreas Enge, Matthieu Finiasz, Caroline Fontaine, Pierre-Alain Fouque, Philippe Gaborit, Pierrick Gaudry, Henri Gilbert, Johan P. Hansen, Éliane Jaulmes, Shaoquan Jiang, Lars R. Knudsen, Emil Kolev, Ivan Landjev, Antoine Lobstein, Samuel Maffre, Gwenaelle Martinet, Jean-Francois Misarsky, Håvard Raddum, Hugues Randriambololona, Robert Rolland, Massimiliano Sala, Hong-yeop Song, Martijn Stam, Cedric Tavernier, Carsten Thomassen, Emmanuel Thomé, Jean-Pierre Tillich, Jacques Traore, Jacques Wolfmann et Viktor V. Zyablov* pour leur précieuse collaboration.

Nous souhaitons également remercier tous les organisateurs, notamment Chantal Girodon et Dominique Potherat. C'est grâce à la contribution de tous, à l'INRIA et à nos soutiens financiers, qu'il nous a été possible de financer un certain nombre de conférenciers.

Nous vous souhaitons un bon séjour à Rocquencourt et un workshop passionnant.

Pascale Charpin et Gregory Kabatiansky,
Présidents du comité de programme.

[1]INRIA: Institut National de Recherche en Informatique et Automatique

**Foreword**

We are pleased to welcome you to this third International Workshop on Coding and Cryptography at the research unit INRIA-ROCQUENCOURT[2].

This foreword gives us the opportunity to thank all the members of the program committee for their great work of reviewing. All 107 submitted abstracts have been reviewed by two referees. Finally, 51 papers have been accepted.

For some papers, the members of the program committee have received help from other researchers. Let me thank *Ali Akhavi, François Arnault, Bram van Asch, Magali Bardet, Peter Beelen, Peter Biyvalenkov, Sebastien Canard, Anne Canteaut, Gerard Cohen, Andreas Enge, Matthieu Finiasz, Caroline Fontaine, Pierre-Alain Fouque, Philippe Gaborit, Pierrick Gaudry, Henri Gilbert, Johan P. Hansen, Éliane Jaulmes, Shaoquan Jiang, Lars R. Knudsen, Emil Kolev, Ivan Landjev, Antoine Lobstein, Samuel Maffre, Gwenaelle Martinet, Jean-Francois Misarsky, Håvard Raddum, Hugues Randriambololona, Robert Rolland, Massimiliano Sala, Hong-yeop Song, Martijn Stam, Cedric Tavernier, Carsten Thomassen, Emmanuel Thomé, Jean-Pierre Tillich, Jacques Traore, Jacques Wolfmann and Viktor V. Zyablov* for their precious help.

We wish also to thank all organizers, in particular Chantal Girodon and Dominique Potherat. Thanks to all of them, to INRIA and to our sponsors, we could support all authors who needed help to attend the workshop.

We wish you a very pleasant stay in Rocquencourt and an exciting workshop!

Pascale Charpin and Gregory Kabatiansky,
Program Chairs

[2]INRIA : FRENCH NATIONAL INSTITUTE OF COMPUTER SCIENCE AND CONTROL

# Contributions

51 *Restrictions on Two-Weight Projective Linear Codes.* Wood J. A 453

**Index**