

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. Helleseeth 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-ROCQUENCOURT¹. 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, Eliane 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.

¹INRIA: 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-ROCQUENCOURT².

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-François 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

²INRIA : FRENCH NATIONAL INSTITUTE OF COMPUTER SCIENCE AND CONTROL

Contributions

1	<i>Negacyclic Codes of Even Length over Z_4.</i> Abualrub T, Abukhaled M	5
2	<i>A Randomized Efficient Algorithm for DPA Secure Implementation of Elliptic Curve Cryptosystems.</i> Agagliate S, Guillot P, Orcière O	11
3	<i>A coding theory bound and zero-sum square matrices.</i> Alon N, Litsyn S, Yuster R	21
4	<i>Codes and designs in Grassmannian spaces.</i> Bachoc C	29
5	<i>Designs and self-dual codes with long shadows.</i> Bachoc C, Gaborit P	35
6	<i>Cryptanalysis of a Provable Secure Additive and Multiplicative Privacy Homomorphism.</i> Bao F	43
7	<i>Distance Distribution of Binary Codes and the Error Probability of Decoding.</i> Barg A, McGregor A	51
8	<i>Two-dimensional array codes correcting 2×2 clusters of errors.</i> Boyarinov I. M	63
9	<i>Fine-Grained Forward-Secure Signature Schemes without Random Oracles.</i> Camenisch J, Koprowski M	71
10	<i>List Signature Schemes and Application to Electronic Voting.</i> Canard S, Traoré J	81
11	<i>Normal and Non Normal Bent Functions.</i> Canteaut A, Daum M, Dobbertin H, Leander G	91
12	<i>Geometrical Cryptography.</i> Csirmaz L, Katona G. O. H	101
13	<i>On Cheating-Immune Secret Sharing.</i> D'Arco P, Kishimoto W, Stinson D	111
14	<i>Trace representation and linear complexity of binary e-th residue sequences.</i> Dai Z., Gong G, Song H. Y	121
15	<i>An Algorithm for Checking Normality of Boolean Functions.</i> Daum M, Dobbertin H, Leander G	133
16	<i>Unconditionally Secure Hierarchical Key Assignment Schemes.</i> De Santis A, Ferrara A. L, Masucci B	143
17	<i>Entity Authentication Schemes Using Braid Word Reduction.</i> Dehornoy P, Girault M, Sibert H	153
18	<i>Provably Secure Non-Interactive Key Distribution Based on Pairings.</i> Dupont R, Enge A	165
19	<i>Fast Gröbner. Algebraic cryptanalysis of HFE and Filter Generators.</i> Faugère J. C	175
20	<i>Results on linear codes meeting the Griesmer bound from results on t-fold $(N - K)$-blocking sets in $PG(N, q)$.</i> Ferret S, Storme L, Sziklai P, Weiner Zs	177
21	<i>Weighted $\{\delta(p^3 + 1), \delta; 3, p^3\}$-minihypers and related linear codes meeting the Griesmer bound.</i> Ferret S	185
22	<i>On the Complexity of Suboptimal Decoding for List and Decision Feedback Schemes.</i> Freudenberger J, Zyablov V	193
23	<i>Transposed rank codes based on symmetric matrices.</i> Gabidulin E. M, Pilichuk N. I	203

24	<i>An efficient semantically secure elliptic curve cryptosystem based on KMOV.</i> Galindo D, Martín S, Morillo P, Villar J	213
25	<i>On-line/off-line RSA-like.</i> Girault M, Paillès J. C	223
26	<i>Homomorphic public-key cryptosystems and encrypting boolean circuits.</i> Grigoriev Y, Ponomarenko I	233
27	<i>Bounds on the error-correction capability of codes beyond half the minimum distance.</i> Helleseth T, Kløve T, Levenshtein V	243
28	<i>Weak Collision Resistance for Variable Input Length Can Imply Collision Resistance for Fixed Input Length.</i> Hirose S, Yoshida S	253
29	<i>On identification of sets of vertices in the triangular grid.</i> Honkala I, Laihonon T	265
30	<i>Affinity of Permutations of \mathbb{F}_2^n.</i> Hou X. D	273
31	<i>Polynomial Interpolation of Cryptographic Functions Related to the Diffie-Hellman Problem.</i> Kiltz E, Winterhof A	281
32	<i>The Generalized Preparata Codes Over $GF(2^l)$.</i> Kuzmin A. S, Markov V. T, Nechaev A. A, Neljubin A. S	289
33	<i>An Explicit Construction of a Class of Good Codes and Their Duals.</i> Ling S, Özbudak, Xing C	299
34	<i>Secret sharing schemes on sparse homogeneous access structures with rank three.</i> Martí-Farré J, Padró C	307
35	<i>Self-dual Extended Group Codes.</i> Martinez-Perez C, Willems W	317
36	<i>A Case When Three Weights in a Cyclic Code is Impossible.</i> McGuire G	323
37	<i>A Wrap Error Attack against NTRUEncrypt.</i> Meskanen T, Renvall A	327
38	<i>Applying General Access Structure to Metering Schemes.</i> Nikov V, Nikova S, Preneel B, Vandewalle J	337
39	<i>Fast Generation of Elliptic Curves with Prime Order over F_{p^2}.</i> Nogami Y, Morikawa Y	347
40	<i>Recovering a Parent Code for Subcodes of Maximal Rank Distance Codes.</i> Ourivski A	357
41	<i>A Maiorana-McFarland type Construction for Resilient Boolean Functions on n Variables (n Even) with Nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$.</i> Pasalic E, Maitra S	365
42	<i>Kernels of q-ary 1-perfect codes.</i> Phelps K. T, Rifa J, Villanueva M	375
43	<i>Some subsets of points in the plane associated to truncated Reed-Muller codes with good parameters.</i> Quarez R	383
44	<i>On the generalized Hamming weights of Hyperelliptic codes.</i> Ramirez-Alzola D	389
45	<i>On the nonlinearity of Boolean functions.</i> Rodier F	397
46	<i>Irreducible Goppa codes.</i> Ryan J, Fitzpatrick P	407
47	<i>Repeated-root cyclic and negacyclic codes over a finite chain ring.</i> Sălăgean A	417
48	<i>Tilings of closed surfaces by Steiner triple systems.</i> Soloveva F	425
49	<i>The Berlekamp-Massey Algorithm and Combinatorics.</i> Tamm U	433
50	<i>Partial reconstruction of perfect binary codes.</i> Vasil'eva A. Y.	445

Index

- Abualrub, T, 5
Abukhaled, M, 5
Agagliate, S, 11
Alon, N, 21
Bachoc, C, 35
Bachoc, C, 29
Bao, F, 43
Barg, A, 51
Boyarinov, I. M, 63
Camenisch, J, 71
Canard, S, 81
Canteaut, A, 91
Csirmaz, L, 101
D'Arco, P, 111
Dai, Z., 121
Daum, M, 133
Daum, M, 91
De Santis, A, 143
Dehornoy, P, 153
Dobbertin, H, 133
Dobbertin, H, 91
Dupont, R, 165
Enge, A, 165
Faugère, J. C, 175
Ferrara A. L, 143
Ferret, S, 185
Ferret, S, 177
Fitzpatrick, P, 407
Freudenberger, J, 193
Gabidulin, E. M, 203
Gaborit, P, 35
Galindo, D, 213
Girault, M, 223
Girault, M, 153
Gong, G, 121
Grigoriev, Y, 233
Guillot, P, 11
Helleseth, T, 243
Hirose, S, 253
Honkala, I, 265
Hou, X. D, 273
Katona, G. O. H, 101
Kiltz, E, 281
Kishimoto, W, 111
Kløve, T, 243
Koprowski, M, 71
Kuzmin, A. S, 289
Laihonen, T, 265
Leander, G, 133
Leander, G, 91
Levenshtein, V, 243
Ling, S, 299
Litsyn, S, 21
Maitra, S, 365
Markov V. T, 289
Martí-Farré, J, 307
Martín, S, 213
Martinez-Perez, C, 317
Masucci, B, 143
McGregor, A, 51
McGuire, G, 323
Meskanen, T, 327
Morikawa, Y, 347
Morillo, P, 213
Nechaev A. A, 289

Neljubin A. S,	289	Sibert, H,	153
Nikov, V ,	337	Soloveva, F,	425
Nikova, S,	337	Song, H. Y,	121
Nogami, Y,	347	Stinson, D,	111
Orcière, O,	11	Storme, L,	177
Ourivski, A,	357	Sziklai, P,	177
Özbudak,	299	Tamm, U,	433
Padró, C ,	307	Traoré, J,	81
Paillès, J. C,	223	Vandewalle, J,	337
Pasalic, E,	365	Vasil'eva, A. Y.,	445
Phelps, K. T,	375	Villanueva, M,	375
Pilichuk, N. I,	203	Villar, J,	213
Ponomarenko, I,	233	Weiner, Zs,	177
Preneel, B,	337	Willems, W,	317
Quarez, R,	383	Winterhof, A,	281
Ramirez-Alzola, D,	389	Wood, J. A,	453
Renvall, A,	327	Xing, C,	299
Rifa, J,	375	Yoshida, S,	253
Rodier, F,	397	Yuster, R,	21
Ryan, J,	407	Zyablov, V,	193
Sălăgean, A,	417		