Arithmetic, Geometry, Cryptography and Coding Theory 2011

Yves Aubry

Christophe Ritzenthaler

Alexey Zykin

Institut de Mathématiques de Toulon, Institut de Mathématiques de Luminy
Current address: Avenue de l'université, 83 957 La Garde Cedex, France; Campus de Luminy, Case 907, 13288 Marseille Cedex 9, France
E-mail address: `aubry@iml.univ-mrs.fr`

Institut de Mathématiques de Luminy
Current address: Campus de Luminy, Case 907, 13288 Marseille Cedex 9, France
E-mail address: `ritzenth@iml.univ-mrs.fr`

State University Higher School of Economics, Laboratory of Algebraic Geometry and its Applications of HSE, Laboratoire J.-V. Poncelet (UMI 2615), Intitute for Information Transmission Problems
Current address: 117312, Vavilova, 7, Moscow, Russia
E-mail address: `alzykin@gmail.com`

2010 *Mathematics Subject Classification.* 11G10, 11G20, 11M38, 11R42, 11T06, 11T71, 14G10, 14G15, 14G50, 14Q05

Contents

Preface

The 13-th $\mathsf{AGC^2T}$ conference (Arithmetic, Geometry, Cryptography and Coding Theory) took place at CIRM (Centre International de Rencontres Mathématiques) in Marseille, France, on March 14–18, 2011. This international conference has been a major event in the area of arithmetic geometry and its applications for more than 25 years and more than 80 participants attended it this year. We thank all of them for creating a stimulating research environment. The topics of the talks extended from algebraic number theory to diophantine geometry, curves and abelian varieties over finite fields and applications to codes, boolean functions or cryptography. We especially thank the speakers Bruno Anglès, Stéphane Ballet, Burcu Baran, Régis Blache, Ivan Boyer, Nils Bruin, Alain Couvreur, Frédéric Edoukou, Arnaldo Garcia, Sudhir Ghorpade, Safia Haloui, Marc Hindry, Masaaki Homma, Everett Howe, Kamal Khuri-Makdisi, David Kohel, Aristides Kontogeorgis, Philippe Langevin, Gregor Leander, Elodie Leducq, Petr Lisonek, Kit-Ho Mak, Alina Ostafe, Ferruh Ozbudak, François Rodier, Karl Rökaeus, Cécilia Salgado, Jean-Pierre Serre, Vijaykumar Singh, Benjamin Smith, Henning Stichtenoth, Bianca Viray, Gabor Wiese and Yuri Zarhin for their lectures.

For the second time, the $\mathsf{AGC^2T}$ conference was twinned with Geocrypt (conference on Geometry and Cryptography) which took place in la Marana near Bastia, Corsica, France, on June 19–24, 2011. This conference focuses on algebraic geometry issues raised by cryptography. We would like to thank Christophe Arene, Xavier Caruso, Luca de Feo, Pierre Dèbes, Oumar Diao, Everett Howe, David Kohel, Reynald Lercier, Pascal Molin, Damien Robert, David Roe, Éric Schost, Benjamin Smith, Peter Stevenhagen, Marco Streng, Emmanuel Thom and Osmanbey Uzunkol for their talks. We also thank the ANR CHIC (Hyperelliptic Curves Isogenies, Point Counting) for its financial support.

The editors would like to thank the staff of CIRM (Olivia Barbarroux, Muriel Milton and Laure Stefanini) and that of the Institut de Mathématiques de Luminy (Aurélia Lozingot and Corinne Roux) for their remarkable professionalism.

Finally, special thanks to the Saint Patrick's day which gave us an opportunity of a memorable party.