EUROPEAN SCIENCE FOUNDATION
SETTING SCIENCE AGENDAS FOR EUROPE

Exploratory Workshop Scheme

Standing Committee for Physical and Engineering Sciences (PESC)

ESF Exploratory Workshop on

CURVES, CODING THEORY, AND CRYPTOGRAPHY

Marseille (France) 26-28 March 2009

Convened by:
David Kohel, Gilles Lachaud and Christophe Ritzenthaler

SCIENTIFIC REPORT

Executive summary

Algebraic curves entered into coding theory in the 1980's with Goppa's introduction of algebraic geometric codes. The proposal of elliptic curves for use in cryptography by Koblitz and Miller in 1985 culminated new elliptic curve-based cryptographic U.S. government standards in 2005. This workshop united researchers actively working on the computational aspects of curves, in order to explore interdisciplinary research and applications to coding theory and cryptography.

The relation between arithmetic geometry, particularly the arithmetic of algebraic curves, coding theory, and cryptography is one of the most fruitful areas of contemporary mathematics. Since the introduction, in 1980's, of the theory of algebraic-geometric codes by Goppa and of elliptic curves to cryptography by Koblitz and Miller, the study of curves over finite fields has seen an explosion of interest. This interest has seen significant advances in the theoretical algorithms and in high-level computational tools for working with curves, codes, and cryptography.

The last decade has seen many advances in algorithms for addressing arithmetic questions concerning the arithmetic of curves : from determining rational points on curves and Mordell-Weil groups of Jacobians over global fields to techniques for discrete logarithms and point counting over finite fields.

This exploratory workshop brought together 28 researchers involved in computational and algorithmic aspects of algebraic curves and their applications. The workshop was structured to have three expository presentations on the state of the art in the morning, with working groups to discuss open research problems in the afternoons, reuniting for closing discussions and group presentations.

This workshop preceded the conference on *Arithmetic, Geometry, Cryptography, and Codimg Theory 12* (AGCT), which took place in 30 March to 3 April 2009 at the *Centre International de Rencontres Mathématiques* (CIRM). This biennial conference gathers together researchers whose interests in geometric aspects of coding theory, random sequences, and cryptography. Discussions began at the Exploratory Workshop (among a subset of the AGCT participants) set the stage for research and discussions over the course of the following week (and thereafter).

Scientific content

The Exploratory Workshop Curves, Coding Theory, and Cryptography took place from 26-28 June 2009, at the Institut de Mathématiques de Luminy. The workshop was structured to have featured expository talks in the morning sessions on the state of the art on select topics. Afternoon sessions were dedicated to organized working groups, and group presentations or reports provided a mechanism for sharing open problems and ideas with the larger audience.

The first day opened with a talk by Dan Bernstein and Tanja Lange (Einhoven) on recent developments in using new models for elliptic curves to achieve better performance in cryptography. This traced recent developments on using alternative equations, or models, for elliptic curves to achieve more efficient arithmetic. This work is particularly important for cryptographic applications in embedded systems like smart cards or mobile telephony.

Gabriele Nebe (Aachen) reported on new algorithms for computing automorphism groups of codes. This has played a key role in determining invariants of boolean functions in cryptography. Patrick Sol\'e (Nice) presented a talk on computational aspects of codes and lattices.

Working groups on elliptic curves, low genus curves, modular forms, p-adic methods, and funtion fields and codes were organized prior to lunch. These groups convened in the afternoon to develop common research questions for presentation before closure of the day's events.

The second day began with a presentation by organizer Christophe Ritzenthaler of joint work with Enric Nart (Barcelona) on new results problems and open problems for genus 3 curves (over finite fields). This was followed by two talks on modular forms by Gabor Wiese (Essen), who reported on an open repository of code for computing with modular forms, and Ian Kiming (Copenhagen),describing open problems for mod p^n modular forms. The working groups were reconstituted and reconvened in the afternoon with reports at the end of the day.

The third day featured a talk by Claus Diem (Leipziq) on state of knowledge for the discrete logarithm problem on plane curves. Understanding the computational complexity of this problem is central to calibrating the security of curve-based cryptography, in order to optimize the efficiency of such systems. This was followed by two talks on p-adic methods in counting points on curves, by Henrik Hubrechts (Leuven) and Ralf Gerkmann(Mainz). These algorithms play a role in finding and constructing secure curves for cryptography and the methods have an intrinsic mathematical interest.

The mathematical programme concluded in the afternoon with discussion of the suitability of various follow-up activities, in particular European networks. The social programme was completed with a traditional French dinner.

Assessment of results

The uniform response from participants was that the workshop was a success. The workshop provided an opportunity for the introduction and interaction of young and established researchers spanning mathematics, computer science and applications. The majority of participants attended the conference AGCT in CIRM during the week which followed the Exploratory Workshop (joined by some 50 additional participants). Research discussions continued into the following week during this conference, and several research projects continue, with articles in preparation and subsequent research visits to Luminy scheduled.

Work presented or developed at this workshop is eligible for submission and inclusion in the (refereed) proceedings of the AGCT. Discussions of potential European research or training networks is ongoing.

Programme

Wednesday 25 March 2009

Evening	*Arrival (Hotel Citadines Castellane)*

Thursday 26 March 2009

09.30-09.40	**Welcome by Convenor** **David Kohel** (Institut de Mathématiques de Luminy)
10.00-12.30	**Morning Session: Coding theory and curves**
10.00-11.00	**Elliptic curve models** **Dan Bernstein** (University of Illinois at Chicago) and **Tanja Lange** (Technische Universiteit Eindhoven)
11.00-11.15	*Coffee / Tea Break*
11.15-12.00	**Automorphism groups of codes** **Gabriele Nebe** (RWTH Aachen)
12.00-12.30	**Codes and lattices** **Patrick Sole** (CNRS, Sophia Antipolis)
12.30-14.00	*Lunch*
14.00-17.30	**Afternoon Session: Working groups**
14.00-15.30	**Discussion and working groups**
15.30-16.00	*Coffee / tea break*
16.00-17.30	**Group reports / presentations**

Friday 27 March 2009

09.30-12.30	**Morning Session: Arithmetic of curves**
09.30-10.15	**Old and new problems on genus 3 curves** **Christophe Ritzenthaler** (Institut de Mathématiques de Luminy)
10.15-10.45	*Coffee / Tea Break*
10.45-11.30	**Computing with modular forms** **Gabor Wiese** (Universität Duisburg-Essen)
11.45-12.30	**Mod p^m modular forms:** **A level reduction result and computational problems** **Ian Kiming** (Københavns Universitet)
12.30-14.00	*Lunch*
14.00-17.30	**Afternoon Session: Working groups**
14.00-15.30	**Discussion and working groups**
15.30-16.00	*Coffee / tea break*
16.00-17.30	**Group reports / presentations**

Saturday 28 March 2009

09.30-12.30	**Morning Session: Curves and cryptography**
09.30-10.15	**On the discrete logarithm problem for plane curves** **Claus Diem** (Universität Leipzig)
10.15-10.45	*Coffee / Tea Break*
10.45-11.30	**Overview of p-adic deformation methods** **Ralf Gerkmann** (Johannes Gutenberg-Universität Mainz)
11.45-12.30	**Point counting using deformation** **Hendrik Hubrechts** (Katholieke Universiteit Leuven)
12.30-14.00	*Lunch*
14.00-17.30	**Afternoon Session: Working groups**
14.00-15.30	**Discussion and working groups**
15.30-16.00	*Coffee / tea break*
16.00-17.30	**Group reports / presentations**
19.30	*Workshop dinner (Les Arcenaulx)*

List of participants

Convenors:

1. **David KOHEL**
   Institut de Mathématiques de Luminy
   Campus de Luminy, Case 907
   13288 Marseille Cedex 9
   France
   kohel@iml.univ-mrs.fr

2. **Gilles LACHAUD**
   Institut de Mathématiques de Luminy
   Campus de Luminy, Case 907
   13288 Marseille Cedex 9
   France
   lachaud@iml.univ-mrs.fr

3. **Christophe RITZENTHALER**
   Institut de Mathématiques de Luminy
   Campus de Luminy, Case 907
   13288 Marseille Cedex 9
   France
   ritzenth@iml.univ-mrs.fr

Participants:

4. **Alp BASSA**
   EPFL SB IMB CSAG,
   Batiment MA, Station 8
   CH-1015 Lausanne
   Switzerland
   alp.bassa@epfl.ch

5. **Daniel BERNSTEIN**
   Department of Computer Science
   University of Illinois at Chicago
   851 S. Morgan Street
   Chicago, IL 60607-7053
   United States
   djb@cr.yp.to

6. **Robert CARLS**
   University of Ulm
   Institute of Pure Mathematics
   D-89069 Ulm
   Germany
   robert.carls@uni-ulm.de

7. **Nils BRUIN**
   Department of Mathematics
   Simon Fraser University
   Burnaby, BC
   Canada V5A 1S6
   nbruin@sfu.ca

8. **John CREMONA**
   Mathematics Institute
   Zeeman Building
   University of Warwick
   Coventry CV4 7AL
   United Kingdom
   john.cremona@gmail.com

9. **Claus DIEM**
   University of Leipzig
   Faculty for Mathematics and Informatics
   Mathematical Institute, Room 01-07
   Johannisgasse 26
   Germany
   Claus.Diem@math.uni-leipzig.de

10. **Claus FIEKER**
    School of Mathematics
    The University of Sydney
    NSW 2006
    Australia
    claus@maths.usyd.edu.au

11. **Ralf GERKANN**
    Institut fur Mathematik (Fachbereich 08)
    Johannes Gutenberg-Universitat Mainz
    Staudingerweg 9
    55099 Mainz
    Germany
    gerkmann@mathematik.uni-mainz.de

12. **David GRUENEWALD**
    School of Mathematics
    The University of Sydney
    NSW 2006
    Australia
    davidg@maths.usyd.edu.au

13. **David HARVEY**
    Department of Mathematics
    Courant Institute
      of Mathematical Sciences
    251 Mercer Street
    New York, NY 10012-1185
    United States
    dmharvey@cims.nyu.edu

14. **Hendrik HUBRECHTS**
    Departement Wiskunde
    Katholieke Universiteit Leuven
    Celestijnenlaan 200b - bus 2400
    3001 Heverlee
    Belgium
    Hendrik.Hubrechts@wis.kuleuven.be

15. **Kiran KEDLAYA**
    Department of Mathematics, Room 2-165
    Massachusetts Institute of Technology
    77 Massachusetts Avenue
    Cambridge, MA 02139
    United States
    kedlaya@mit.edu

16. **Ian KIMING**
    Institut for Matematiske Fag
    Københavns Universitet
    Universitetsparken 5
    DK-2100 Copenhagen Ø
    Denmark
    kiming@math.ku.dk

17. **Tanja LANGE**
    Department of Mathematics
      and Computer Science
    Room HG 9.92
    Technische Universiteit Eindhoven
    P.O. Box 513
    5600 MB Eindhoven
    Netherlands
    tanja@hyperelliptic.org

18. **Philippe LEBACQUE**
    School of Mathematical Sciences
    University of Nottingham
    University Park
    NG7 2RD Nottingham
    United Kingdom
    Philippe.Lebacque@nottingham.ac.uk

19. **Stephen MEAGHER**
    Department of Mathematics
    Albert-Ludwigs-University Freiburg
    Eckerstrasse 1, Room 434
    79104 Freiburg im Breisgau
    Germany
    Stephen.Meagher@math.uni-freiburg.de

20. **Gary MCGUIRE**
    UCD School of Mathematical Sciences
    Science Education and Research Centre
    University College Dublin
    Belfield, Dublin 4
    Ireland
    gary.mcguire@ucd.ie

21. **Enric NART**
    Departament de Matematiques
    Edifici C
    Universitat Autonoma de Barcelona
    08193 Bellaterra (Barcelona)
    Spain
    nart@mat.uab.cat

22. **Gabriele NEBE**
    Lehrstuhl D fur Mathematik
    RWTH Aachen
    Templergraben 64
    52062 Aachen
    Germany
    nebe@math.rwth-aachen.de

23. **Rene SCHOOF**
    Universita di Roma Tor Vergata
    Dipartimento di Matematica
    Via della Ricerca Scientifica
    I-00133 Roma
    Italy
    schoof@mat.uniroma2.it

24. **Ben SMITH**
    Laboratoire d'informatique (LIX)
    Ecole polytechnique
    91128 Palaiseau cedex
    France
    smith@lix.polytechnique.fr

25. **Patrick SOLE**
    Laboratoire I3S UNSA-CNRS
    Polytech'Nice
    930 route des Colles
    BP.145
    06903 Sophia Antipolis - Cedex
    France
    ps@essi.fr

26. **Katherine STANGE**
    Department of Mathematics
    Harvard University
    One Oxford Street
    Cambridge MA 02138
    stange@math.harvard.edu

27. **Gabor WIESE**
Institut fur Experimentelle Mathematik
Universitat Duisburg-Essen
Ellernstr. 29
D-45326 Essen
Germany
gabor.wiese@uni-due.de

28. **Alexey ZAYTSEV**
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4
Ireland
alexey.zaytsev@ucd.ie

Statistical information on participants

The workshop brought together 28 participants, including organisers, with broad participation from across Europe as well as international participants:

Germany : 6	Belgium : 1
France : 5	Canada : 1
United States : 3	Denmark : 1
Australia : 2	Italy : 1
Ireland : 2	Spain : 1
Netherlands : 2	Switzerland : 1
UK: 2	

There was strong representation of young researchers, 12 of whom were less than five years from completion of their PhD.