

Euler Institute for Discrete Mathematics and its  
Applications  
ANNUAL REPORT 2004



## Preface

The year 2004 was not the easiest year for EIDMA. On September 28, Prof. Jack van Lint passed away. He inspired us more than ten years ago to establish EIDMA as a research school. Many view him as the founding father of Discrete Mathematics in the Netherlands, may be even in Europe. The Executive Council of the TU/e decided no longer to support EIDMA (nor any other research school). The Board of Governors of EIDMA is developing alternative ways of financing. Finally, the Discrete Mathematics group in Delft was discontinued and had to terminate its membership.

But there is also good news. In November 2003, the Crypto Group of the Université Catholique de Louvain led by Prof. Jean-Jacques Quisquater, joined EIDMA. This will strengthen our activities in information security. Noteworthy is also that Prof.dr. A.E. Brouwer received a honorary doctorate from the University of Aalborg, that Prof.dr. G.R. Woeginger received a VICI award and that Prof.dr.ir. K.A. Schouhammer-Immink received the SMPTE Progress Medal, the IEEE Consumer Electronics Engineering Excellence Award and was the Heyser Memorial lecturer. Thirteen Ph.D. students successfully defended their thesis.

EIDMA is proud that it could continue its tradition of offering world-class mini-courses:

- Prof. Éva Tardos, Cornell University, USA.  
Approximation Algorithms and Games on Networks.
- Prof. Bernhard Mühlherr, Université Libre de Bruxelles, Belgium.  
Building and Groups of Lie Type.
- Prof. Joachim Hagenauer, TU München, Germany, and Prof. Rüdiger Urbanke, Swiss Federal Institute of Technology, Switzerland.  
Iterative Decoding Techniques.

In 2004, EIDMA also started preparations for the procedure to be accredited again by the KNAW. The on-site visit by the peer reviewers (Prof. A.R. Calderbank, Prof. P. Fitzpatrick, Prof. C.J.H. McDiarmid and Prof. T. Helleseth) seemed to be successful and is reason to remain optimistic for the future.

Prof.dr.ir. H.C.A. van Tilborg  
Scientific Director



# Contents

<b>1</b>	<b>Structure and Composition of EIDMA</b>	<b>7</b>
1.1	Organizational Structure . . . . .	7
1.2	Participating Groups . . . . .	8
<b>2</b>	<b>EIDMA courses, seminars and meetings in 2004</b>	<b>12</b>
<b>3</b>	<b>Research Activities</b>	<b>13</b>
3.1	Discrete Algebra and Geometry . . . . .	14
3.1.1	Ruhr-Universität Bochum, Germany, Horst-Görtz-Institut für IT Sicherheit . . . . .	14
3.1.2	Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Discrete Mathematics Group . . . . .	16
3.1.3	Université Libre de Bruxelles, Belgium, Département de Mathématique . . . . .	17
3.1.4	Universiteit Gent, Belgium, Dept. of Applied Mathematics and Computer Science, Group Combinatorial Algorithms and Algorithmic Graph Theory . . . . .	18
3.1.5	Universiteit Gent, Belgium, Department of Pure Mathematics and Computer Algebra, Research Group Incidence Geometry . . . . .	18
3.1.6	Universiteit van Tilburg, Faculty of Economics and Business Administration, Econometrics and Operations Research Group . . . . .	20
3.2	Coding Theory, Information Theory and Cryptology . . . . .	20
3.2.1	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Nationaal Bureau voor Verbindingsbeveiliging, Den Haag	20
3.2.2	Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Discrete Mathematics Group . . . . .	21
3.2.3	Technische Universiteit Eindhoven, Department of Electrical Engineering, Information and Communication Systems Group . . . . .	23
3.2.4	TNO Information and Communication Technology, Delft	24
3.2.5	Universiteit Gent, Belgium, Department of Pure Mathematics and Computer Algebra, Research Group Incidence Geometry . . . . .	24
3.2.6	Université Catholique de Louvain, Belgium, UCL Crypto Group . . . . .	24
3.3	Combinatorial Optimization, Combinatorial Algorithms and Graph Theory . . . . .	25
3.3.1	Centrum voor Wiskunde en Informatica, Amsterdam, Group Networks and Logic - Optimization and Program- ming . . . . .	25
3.3.2	Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Combinatorial Optimization Group . . . . .	27
3.3.3	Université Libre de Bruxelles, Belgium, Département de Mathématique . . . . .	30
3.3.4	Universiteit Gent, Belgium, Dept. of Applied Mathematics and Computer Science, Group Combinatorial Algorithms and Algorithmic Graph Theory . . . . .	30

3.3.5	Universiteit Twente, Faculty of Mathematical Sciences, Group Discrete Mathematics and Mathematical Program- ming . . . . .	31
<b>4</b>	<b>Publications in 2004</b>	<b>34</b>
4.1	Books . . . . .	34
4.2	Research articles in refereed journals . . . . .	34
4.3	Research articles awaiting publication . . . . .	43
4.4	Research articles submitted for publication . . . . .	50
4.5	Conference Proceedings . . . . .	53
4.6	Preprints and Internal Reports . . . . .	61
4.7	Patents . . . . .	64
<b>5</b>	<b>Lectures in 2004</b>	<b>65</b>
<b>6</b>	<b>External Grants in 2004</b>	<b>80</b>
<b>7</b>	<b>Noteworthy Activities in 2004</b>	<b>82</b>
7.1	Awards . . . . .	82
7.2	Ph.D. Degrees . . . . .	82
7.3	Ph.D. Committees . . . . .	85
7.4	Editorships . . . . .	88
7.5	Organization of workshops and conferences . . . . .	91
7.6	Memberships . . . . .	94

# 1 Structure and Composition of EIDMA

## 1.1 Organizational Structure

- Board of Governors:
  - Prof.dr. A.M. Cohen, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science (chairman).
  - Dr. T.S.H. Driessen, Universiteit Twente, Faculty of Mathematical Sciences (*as of February 1, 2004*).
  - Prof.dr. A. Schrijver, Centrum voor Wiskunde en Informatica.
  - Dr. J. Simonis, Technische Universiteit Delft, Faculty of Information Technology and Systems (*till May 1, 2004*).
  - Dr. F.M.J. Willems, Technische Universiteit Eindhoven, Department of Electrical Engineering.
  - Prof.dr. G.J. Woeginger, Universiteit Twente, Faculty of Mathematical Sciences (*till February 1, 2004*).
- Scientific Director: Prof.dr.ir. H.C.A. van Tilborg, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science.
- Secretary: Ir. H.J.M. Wijers, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science.
- Management assistant: mrs. H.A.M. Houben-Verhees, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science.
- Scientific Board:
  - Prof.dr. E.H.L. Aarts, TU Eindhoven and Philips Research, Eindhoven (chairman).
  - Ir. M.J.M.M. van Asperdt, NBV, Den Haag.
  - Dr.ir. C.P.M.J. Baggen, Philips Research, Eindhoven.
  - Prof.dr. A.E. Brouwer, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science.
  - Dr. Ph. Cara, Université Libre de Bruxelles, Department of Mathematics, Belgium.
  - Prof.dr. H. Dobbertin, Horst-Görtz Institute, Bochum, Germany.
  - Prof.dr. J.-J. Quisquater, Université Catholique de Louvain, Crypto Group, Louvain-la-Neuve, Belgium.
  - Dr. G. Sierksma, RU Groningen, QLORG.
  - Dr. L. Stougie, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science (*till February 1, 2004*).
  - Prof.dr. J.A. Thas, Universiteit Gent, Department of Pure Mathematics and Computer Algebra, Belgium.
  - Prof.dr.ir. J.P.L. Vandewalle, Katholieke Universiteit Leuven, Department of Electrical Engineering, Belgium.
  - Prof.dr.ir. A.J. Vinck, Institut für Experimentelle Mathematik, Essen, Germany.
  - Prof.dr. G.J. Woeginger, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science (*as of February 1, 2004*).

## 1.2 Participating Groups

In 2004, EIDMA consisted of the following groups and persons:

### THE NETHERLANDS

- Center for Mathematics and Computer Science (CWI), Amsterdam, Research group "Networks and Logic - Optimization and Programming":
  - Staff members: mrs. dr. K.I. Aardal, prof.dr.ir. A.M.H. Gerards, mrs. dr. M. Laurent, prof.dr. J.K. Lenstra, prof.dr. A. Schrijver, dr. M.R. Cerioli, E. Colin de Verdière, dr. L. Stougie.
  - Post-docs: dr. H. van der Holst, dr. D. Jibeteau, dr. S. Kelk, G. Maróti
  - PhD students: J. Byrka, N. Gvozdenović, W.J. van Hoeve, D.C. Gijswijt.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Nationaal Bureau voor Verbindingsbeveiliging, Den Haag:
  - Staff members: ir. M.J.M.M. van Asperdt, drs. B. Botma, dr.ir. P.A.H. Bours, ir. R.W.M.G. Doijen, ir. L.P. van Drimmelen, drs. J.W.L. Drossaers, drs. E. van der Laan, drs. S. Oudkerk, dr.ir. C.L.M. van Pul, ing. K. van der Raad, ir. G. Roelofsen, ir. G. Schmitz, J.M.J.B. van Zanten.
- Philips Research Laboratories, Eindhoven:
  - Staff members: prof.dr. E.H.L. Aarts, dr.ir. C.P.M.J. Baggen, drs. S. Egener, drs. P. Gorissen, dr.ir. A.P. Hekstra, ir. W.J. van Houtum, Msc. S.A. Husen, dr.ir. H.D.L. Hollmann, ir. F.L.A.J. Kamperman, dr.ir. T.A.M. Kevenaer, ir. A.G.C. Koppelaar, dr.ir. J.H.M. Korst, dr.ir. J.P.M.G. Linnartz, ir. W.P.A.J. Michiels, dr. J.C. Oostveen, ir. S.P.P. Pronk, ir. G.-J. Schrijen, ir. M.L.A. Stassen, J. Talstra, dr.ir. L.M.G.M. Tolhuizen, ir. H.Y. Tsang, dr. P. Tuyls, dr.ir. W.F.J. Verhaegh, dr.ir. A. van der Werf.
- Technische Universiteit Delft, Faculty of Information Technology and Systems, Section Algebra and Geometry (*till May 1, 2004*):
  - Staff members: dr.ir. R. Goldbach, dr.ir. J.G. Maks, dr. J. Simonis, prof.dr.ir. Th.H.M. Smits, prof.dr. A.J. van Zanten.
  - PhD students: L. Haryanto, I. Suparta.
- Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Discrete Mathematics Group:
  - Staff members: dr. A.G. van Asch, dr. A. Blokhuis, prof.dr. A.E. Brouwer, prof.dr. N.G. de Bruijn (em.), prof.dr. A.M. Cohen, dr. F.G.M.T. Cuypers, prof.dr. A.K. Lenstra, prof.dr. J.H. van Lint (em.), dr. G.R. Pellikaan, dr. L.A.M. Schoenmakers, dr. H.J.M. Sterk, prof.dr.ir. H.C.A. van Tilborg, dr. B.M.M. de Weger, dr.ir. H.A. Wilbrink.
  - Post-docs: mrs.dr. D. Jibeteau, dr. M. Lavrauw, dr. S.M. Murray.
  - PhD students: D. Gijbsbers, S. Haller, mrs. E. Jochemsz, M. Kiraz, T. Mussche, M. Nguyen Van Minh, E. Postma, E. Reinaldo Barreiro, R. Rezaeian Farashahi, A. Sidorenko,
- Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Combinatorial Optimization Group:

- Staff members: prof.dr.ir. A.M.H. Gerards, dr.ir. C.A.J. Hurkens, mrs. dr. J.C.M. Keijsper, prof.dr. J.K. Lenstra, dr. R.A. Pendavingh, dr. L. Stougie, prof.dr. G.J. Woeginger.
- PhD students: J. van den Broek, P. Korteweg, R. Sitters.
- Technische Universiteit Eindhoven, Department of Electrical Engineering, Information and Communication Systems Group:
  - Staff members: dr. Tj. Tjalkens, dr.ir. F.M.J. Willems.
  - PhD student: C.K. Ho, T. Ignatenko, A. Martinez.
- TNO Telecom, Delft:
  - Staff members: ir. P. Albeda, ir. F. Fransen, dr.ir. P.J.M. Veugen.
  - PhD students: M. Dekker.
- Universiteit van Tilburg, Faculty of Economics and Business Administration, Econometrics and Operations Research Group:
  - Staff members: dr.ir. E.R. van Dam, dr.ir. W.H. Haemers, dr.ir. M.J.P. Peeters.
- Universiteit Twente, Faculty of Electrical Engineering, Mathematics and Computer Science, Department of Applied Mathematics, Group Discrete Mathematics and Mathematical Programming:
  - Staff members: dr.ir. H.J. Broersma, dr. T.S.H. Driessen, prof.dr. C. Hoede (em.), dr. J.L. Hurink, dr. W. Kern, dr.ir. D. Paulusma, dr.ir. G.F. Post, dr. G.J. Still, prof.dr. G.J. Woeginger.
  - PhD students: P.S. Bonsma, H.E. Baarsma, T. Brueggemann, T. Nieberg, A.N.M. Salman, X. Wang.

## BELGIUM

- Katholieke Universiteit Leuven, Belgium, Department Electrical Engineering (ESAT), Group Computer Security and Industrial Cryptography (COSIC):
  - Staff members: prof.dr.ir. B. Preneel, prof.dr.ir. J. Vandewalle, mrs. prof.dr.ir. I. Verbauwhede.
  - Post-docs: dr.ir. A. Biryukov, dr. K. Kursawe, dr. G. Neven, mrs. dr. S. Nikova, dr. M. Quisquater, dr. J. Scholten, dr. F. Vercauteren.
  - PhD students: mrs. L. Batina, A. Bosselaers, mrs. A. Braeken, C. De Cannière, J. Cappaert, D. De Cock, mrs. M. Deng, mrs. E. Dewitte, mrs. C. Diaz, T. Herlea, J. Lano, R. Maier, mrs. N. Mentens, mrs. E. De Mulder, mrs. B. Örs, dr. M. Quisquater, B. Van Rompay, D. Schellekens, S. Seys, D. Singelee, P. Souradyuti, F. Vercauteren, C. Wolf, K. Wouters, B. Wyseur.
- Université Libre de Bruxelles, Belgium, Département de Mathématique:
  - Graphes et Optimisation Mathématique:
    - \* Staff members: mrs. prof.dr. M. Labbé, prof.dr. M. Van Vyve.
    - \* Post-doc: dr. L. De Giovanni.
    - \* PhD students: mrs. S. Dewez, G. Fasbender, mrs. G. Heilporn, D. Huygens, H. Mélot and A. Özsoy.
  - Service de Géométrie:

- \* Staff members: prof.dr. F. Buekenhout (em.), mrs.dr. C. Cerf, dr. M. Dehon, prof.dr. J. Doyen, prof.dr. D. Leemans, prof.dr. B. Mühlherr.
- \* Post-docs: mrs. dr. A. Devillers, dr. Ph. Cara, dr. M. Sebillé.
- \* PhD students: N. Bougard, P.E. Caprace, mrs. P. Jacobs, mrs. A. Nguyen, mrs. J. De Saedeleer.
- Faculté des Sciences Appliquées:
  - \* Staff members: mrs. prof. A. Delandtsheer.
  - \* Post-docs: dr. C. Archer.
  - \* PhD students: M. Bogaerts, J.-L. Michel.
- Service de Mathématiques et d’Informatique Générales:
  - \* Staff members: prof. J.-P. Doignon.
  - \* Post-docs: dr. S. Fiorini.
  - \* PhD students: mrs. J. Christophe, G. Joret, A. Labarre.
- Laboratoire d’Informatique Théorique:
  - \* Staff member: prof.dr. Y. Roggeman.
- Universiteit Gent, Belgium, Department of Applied Mathematics and Computer Science, Research group Combinatorial Algorithms and Algorithmic Graph Theory:
  - Staff members: prof.dr. G. Brinkmann, prof.dr. K. Coolsaet, mrs. prof.dr. V. Fack.
  - PhD students: mrs. M. Cimráková-Cajková, J. Degraer, D. Van Dyck, J. Winne.
- Universiteit Gent, Belgium, Department of Pure Mathematics and Computer Algebra, Research Group Incidence Geometry:
  - Staff members: prof.dr. F. De Clerck, prof.dr. R. Puystjens, prof.dr. L. Storme, prof.dr. J.A. Thas, prof.dr. H. Van Maldeghem.
  - Post-docs: dr. B. De Bruyn, dr. T. De Medts, dr. P. Govaerts, mrs. dr. E. Kuijken, mrs. dr. D. Luyckx, dr. A. Offer, dr. K. Thas.
  - PhD students: J. De Beule, N. De Feyter, J. De Kaey, mrs. A. De Wispelaere, S. De Winter, mrs. N. Haelvoet, F. Haot, mrs. C. Tonesi, P. Vandecasteele.
- Université Catholique de Louvain, Belgium, UCL Crypto Group (*member as of 24.11.2003*):
  - Staff members: prof. J.-J. Quisquater.
  - Post-docs: dr. F. Koeune, O. Pereira, G. Rouvroy, F.X. Standaert.
  - PhD students: N. Aboudagga, L. Bohy, P. Bulens, J. Cathalo, D. Giry, G. Meurice de Dormale, B. Libert, M. Nève, G. Piret, E. Peeters, D. Samhyde.

## GERMANY

- Ruhr-Universität Bochum, Germany, Horst-Görtz-Institut für IT Sicherheit:
  - Staff members: dr. R.M. Avanzi, prof.dr. H. Dobbertin, prof. C. Paar, prof. A.-R. Sadeghi, prof.dr. J. Schwenk.

- Post-docs: mrs. dr. T. Lange.
- PhD students: A. Adelsbach, M. Daum, P. Felke, S. Kumar, G. Leander, mrs. K. Lemke, M. Manulis, J. Pelzl, K. Schramm, C. Stüble, A. Weimerskirch, M. Wolf, Th. Wollinger.
- Universität Duisburg-Essen, Germany, Institute for Experimental Mathematics, Digital Communications Group:
  - Staff members: prof.dr. K.A.S. Immink, prof.dr. H. Stichtenoth, prof.dr. Trung Van Tran, prof.dr.ir. A.J. Han Vinck.
  - PhD students: O. Meili, P. Svaba.

## 2 EIDMA courses, seminars and meetings in 2004

In 2004, EIDMA organized the following courses, seminars and meetings:

- Minicourses:
  - Prof.Dr.-Ing. Joachim Hagenauer (TU München, Germany) and Dr. Rüdiger Urbanke (Swiss Federal Institute of Technology, Switzerland), *Iterative Decoding Techniques*, TU Eindhoven, February 16–20, 2004.
  - Prof.Dr. B. Mühlherr (Université Libre de Bruxelles, Belgium), *Buildings and Groups of Lie Type*, TU Eindhoven, March 8–12, 2004.
  - Prof.Éva Tardos (Cornell University, USA), *Approximation Algorithms and Games on Networks*, TU Eindhoven, May 10–14, 2004.
- Regular courses:
  - Discrete Algebra and Geometry I (DAG1), March 29–May 4, 2004.
- Seminars:
  - Combinatorial Theory Seminar, Technische Universiteit Eindhoven (every Wednesday afternoon).
  - Seminar Coding, Crypto and Information Theory, Technische Universiteit Eindhoven (2x a year).
  - Cryptography Working Group, Utrecht (4x a year).
  - Optimization Seminar, Technische Universiteit Eindhoven (bi-weekly).
- EIDMA was (co)-organizer / (co)-subsidizer of the following meetings:
  - Nederlands-Belgisch Mathematisch Congres, Universiteit van Tilburg, April 16–17, 2004.
  - Seminar Day Combinatorial Optimization, TU Eindhoven, May 24, 2004.
  - 8th International Workshop on High Performance Optimization Techniques (HPOPT 2004), CWI, Amsterdam, June 23–25, 2004.
  - Conference Incidence Geometry, Conference Center Floreal Club, La Roche, Belgium, May 23–29, 2004.
  - EIDMA 2004 Symposium, Conference Center Carlton De Brug, Mierlo, November 25–26, 2004.

### 3 Research Activities

The research activities of EIDMA concentrate on three main topics:

- Discrete algebra and geometry,
- Coding theory, information theory and cryptology,
- Combinatorial optimization, combinatorial algorithms and graph theory.

We first give a short description of these three areas of research and then, in the subsequent sections, list the contributions of the various research groups in these areas.

#### Discrete algebra and geometry

##### *Design theory*

Existence results, constructions and possible unicity of finite discrete structures with a given specification (often by means of some parameters). The structures can be classical block designs, but also association schemes, mutually orthogonal Latin squares, etc.

##### *Geometry*

The study of the geometry of groups of Lie type, buildings (introduced by Tits) and the diagram geometries of Buekenhout. Constructions, characterizations and classification problems of incidence geometries such as generalized polygons, near polygons, (semi)partial geometries are part of the research activities. Also included are combinatorial problems concerning point sets in finite projective planes and spaces, especially blocking sets and arcs as well as characterizations of quadric and Hermitian Veronese varieties.

##### *Algebra*

The classical relation between algebra and geometry enables the use of algebra to solve geometric problems. In particular need to be mentioned linear algebra, group theory, Clifford algebras and, to a lesser degree, number theory and topology.

##### *Computer-algebraic methods*

Algebra viewed as the study of operations on sets can, when the computer is able to perform these operations, be supported by expert systems, formula-manipulation, searching software, as well as classical computations. The study of the methods to realize this is the focus of this project.

#### Coding theory, information theory and cryptology

##### *Source coding*

Determining the most efficient (shortest) way to represent a certain amount of information. Designing algorithms that realize such a representation.

##### *Channel coding*

Representing an amount of information, that makes reliable transmission possible. Designing algorithms, that realize reliable transmission.

##### *Coding methods for communication networks*

The study of source and channel coding, encoding and addressing (protocols) in networks.

##### *Cryptology*

Protecting information against unauthorized access (privacy), determining if a message has been altered by a third party (integrity), adding a signature to an electronic document and verifying the identity, all by mathematical means.

## **Combinatorial optimization, combinatorial algorithms and graph theory**

### *Algorithms for NP-hard problems*

The development and analysis of optimal and suboptimal algorithms for NP-hard problems.

### *Polynomial algorithms, combinatorics and graph theory*

The design and analysis of optimization algorithms that have a polynomial-bounded complexity. The application of these algorithms.

### *Graph-theoretic problems*

Graph theory deals with a variety of different problems. We mention functions that transform graphs into graphs like line graphs, topics like perfect graphs, cycle coverings of graphs and homomorphisms of graphs, the relation between graphs and cooperative games, and graph theoretic applications in knowledge-technology and social sciences.

A different area concerns the representation of graphs, metric graph theory (with emphasis on shortest paths), the relation between geometric and algebraic structures, applications in discrete location theory and the theory of (dynamic) searching in graphs.

A third area are applications of graph theory and optimization in telecommunication networks.

### *Cycles and paths in graphs*

The existence of Hamilton cycles in graphs and, more general, of cycles and paths with particular properties.

## **3.1 Discrete Algebra and Geometry**

### **3.1.1 Ruhr-Universität Bochum, Germany, Horst-Görtz-Institut für IT Sicherheit**

- Andre Adelsbach:  
Andre Adelsbach works in the research group of Jörg Schwenk. His research interests include cryptographic copyright protection, Digital Rights Management (DRM), cryptographic protocols in general and steganography.
- Magnus Daum:  
Magnus Daum was concerned with an analysis of attacks on hash functions, especially on MD5 and functions of the SHA family. Furthermore he studied the decidability of Boolean functions.
- Hans Dobbertin:  
He worked on the cryptanalysis of hash function and symmetric ciphers. He studied Boolean functions and power functions with high nonlinearity, in particular the construction of bent functions. Further research was focused on weight distributions of cyclic codes, correlation properties of binary sequences and difference sets with Singer parameters. Hereby a main intention was the development of new techniques which allow to handle previously unreachable problems. Moreover, Dobbertin initiated the study of so-called inner collisions as a base of sidechannel attacks. This idea was applied with success for instances by Gregor Leander and Kai Schramm on the AES.

- Patrick Felke:  
Patrick Felke's research was focused on the distribution of the cross-correlation function of sequences and related topics as the problem of computing the uniformity of mappings. He was mainly concerned in niho type cross-correlation functions over finite fields with arbitrary characteristic. Thereby he followed an idea introduced by Dobbertin to reduce this problem to a problem involving the study of Dickson polynomials, but also applied the multi-variate method to determine the distribution. Beside this Patrick Felke was still interested in the cryptanalysis of HFE-systems, especially the systems Sflash and Quartz. He also did some minor work on DPA-attacks against the AES-cryptosystem implemented on a smartcard.
- Sandeep S. Kumar:  
Instruction set extensions which enable public-key algorithms on small microprocessors. In this project he implemented hyperelliptic curves over optimal extension fields on an FPGA. In general he is concerned with cryptography in constrained (low-area and low-power) environments, hardware-Software Co-design for public-key cryptography, and RFID security.
- Tanja Lange:  
Tanja Lange's area of research are curve based cryptography and establishing complexity lower bounds for solving DL (and related systems) using character sums. She developed even more efficient explicit formulae for genus two curves and considered countermeasures against side-channel attacks.
- Gregor Leander:  
Gregor Leander continued his research area in 2002 on bent functions and normal bent functions. During his visit at the Crypto research group in Aarhus, Denmark, from March until May 2002 he worked on Muliparty Computation from Linear Secret Sharing Schemes.
- Kerstin Lemke:  
Kerstin Lemke belongs to Chistof Paar's chair. She works on side-channel attacks and countermeasures.
- Mark Manulis:  
He studies schemes for ad-hoc group communication, key management, anonymity and privacy in IP-multicast and group communication scenarios.
- Christof Paar:  
Christof Paar works on a broad scope of problem - starting from fast algorithms for software implementations they reach to hardware architectures, security of smart cards to applications of IT-security in cars and other embedded systems.
- Jan Pelzl:  
Improving the group operation formulas for cryptosystems based on hyperelliptic curves (HEC), and HEC implementations on embedded processors. Together with Thomas Wollinger he was concerned with implementations of genus two, three and four curves in restricted environments. Furthermore, he started research on hardware for factoring.
- Ahmad-Reza Sadeghi:  
He considers problems from applied and theoretical data security, with

an emphasis on all aspects of DRM, including, trusted computing, secure operation system, and copy right protection. Other areas he works in are protocols and special-purpose hardware.

- Kai Schramm:  
Side-channel attacks on symmetric cipher. He considers a new class of side channel attacks based on internal collisions which he shows to work for DES, AES and other ciphers. He is also applying side-channel techniques to reverse engineering.
- Jörg Schwenk:  
Within the HGI, Jörg Schwenk is the chair for Network Security, in this area he studies IP multicast and groupcommunication layer 2-security. He works on progress on IPSec (e.g. IKEv2). Other topics include XML-security and key management in practice (XML and OpenPGP, XML and S/MIME, XML and X.509-PKIs), pay-TV, Digital Rights Management systems and individual systems for content security.
- Christian Stüble:  
Christian Stüble joint the research group of Ahmad Sadeghi in 2003 where he works on trusted computing and secure operating systems.
- Andr Weimerskirch:  
Protocols which provide security in ad-hoc networks and security in pervasive networks. In this research he also deals with elliptic curve cryptography and efficient protocols. Another area he is active the cryptanalysis of real-world systems.
- Marko Wolf:  
He has finished his diploma in electrical engineering in 2003 and joint the research group of Prof. Paar where he works on robust implementations of cryptographic systems.

### **3.1.2 Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Discrete Mathematics Group**

Within the programme ‘Discrete Algebra and Geometry’, the fundamental motivation is the search for discrete structures with certain required properties. These structures range from nice nice geometries to tournament schemes, from configurations in Euclidean space to abstract finite groups. The main question usually regards existence (alternatively, a proof of nonexistence). Related problems are (efficient) constructions, additional structure (like more symmetry than the required properties suggest), and if applicable, uniqueness. The geometries, groups, graphs, and algebras related to Lie theory are a source of inspiration. A second, more society oriented, goal is to make mathematics more powerful, more accessible and more transparent on computer. We discuss our progress in each of the four strands on which the group focuses, and end with some loose items.

#### **A. Discrete structures**

The research on discrete structures includes the study of special point sets in finite projective planes and spaces, discrete lattices, partial linear spaces and geometries of Lie type, but also statistical designs.

#### **B. Algebras, groups, geometries of Lie type**

Besides various investigations on geometries of Lie type (see also A) and algorithmic aspect of groups of Lie type (see C), also Lie algebras have been topic of research. In particular, geometric aspects of (modular) Lie algebras have been studied. Other topics have been ongoing research in BMW algebras carried out together with David Wales and investigations of subgroups of groups of Lie type generated by special elements.

### C. Algorithms in algebra

Within the area of Algorithms in Algebra, there have been various activities concerning the implementation of abstract groups of Lie type on a computer. In particular, in cooperation with Scott Murray and Don Taylor, a Magma package has been developed that implements the Steinberg presentation of such groups. Moreover, explicit constructions of various forms of algebraic groups of Lie type have been realized and studied.

### D. Mathematics and Computers

This research is conducted with Riaca, the Research Institute of Applications in Computer Algebra, which is located at the TU/e. The research concentrated on the development of interactive mathematical documents. The focus has been on the practical implementation of a context aware system for mathematical documents.

#### 3.1.3 Université Libre de Bruxelles, Belgium, Département de Mathématique

- Service de Géométrie:
  - Nicolas Bourgard: Orbits of automorphism groups: A characterization of the number of orbits of the automorphism groups of various combinatorial structures.
  - Pierre-Emmanuel Caprace: The isomorphism problem for Kac-Moody groups.
  - Philippe Cara: The main themes are incidence geometry and permutation groups. He studies the relation between these two topics via independent sets in finite groups. There was also a project concerning the use of symmetries to optimize parallel computers.
  - Alice Devillers: Structures with highly transitive automorphism groups.
  - Dimitri Leemans: Incidence geometries on which finite (simple) groups act flag-transitively and residually weakly primitively. This involves development of computer programs, also inside the computer algebra package Magma, as well as theoretical work. Abstract polytopes with an emphasis on classifying quotients of universal polytopes.
  - Pascale Jacobs: Development of computer programs to test properties in incidence geometry using the computer algebra package Magma.
  - Bernhard Mühlherr: He is particularly interested in groups acting on buildings which are combinatorial structures introduced by Tits in order to investigate Lie-type groups, groups of Kac-Moody type and Coxeter groups.
  - Aude Nguyen: Geometry, combinatorics and group theory.
- Faculty of Applied Sciences:
  - Prof. Anne Delandtsheer: Designs and groups.

- Dr. Claude Archer: Extensions of groups and incidence geometries.
- Mathieu Bogaerts: Permutation arrays.
- Jean-Luc Michel: Tilings and packings.
- Service de mathématiques et d’informatique générales :
  - Julie Christophe: Facets of polytopes defined from finite affine geometries (joint work with Jean-Paul Doignon).
  - Jean-Paul Doignon: Facets of polytopes defined from finite affine geometries (joint work with Julie Christophe). Transitivity trios of relations (joint work with Jean-Claude Falmagne). Stochastic transitivity (joint work with Mike Regenwetter).
  - Samuel Fiorini: DFacets of 0/1-polytopes, and more specifically of the linear ordering polytope and dicycle cover polytope.

**3.1.4 Universiteit Gent, Belgium,  
Dept. of Applied Mathematics and Computer Science,  
Group Combinatorial Algorithms and Algorithmic Graph Theory**

- Miroslava Cimrkov-Čajkov: Algorithms for exhaustive search for ovoid-like substructures in generalized polygons.
- Kris Coolsaet: Algebraic structure of generalized octagons. Generation and search algorithms in finite geometry.
- Veerle Fack: Generation and search algorithms in finite geometry.
- Joost Winne: Software tools for combinatorial algorithms.

**3.1.5 Universiteit Gent, Belgium,  
Department of Pure Mathematics and Computer Algebra,  
Research Group Incidence Geometry**

- Jan De Beule: Spreads, partial spreads, covers, ovoids and blocking sets of polar spaces. Applications of Computer Algebra in finite geometry.
- Bart De Bruyn: Near polygons, generalized quadrangles, dual polar spaces, distance-regular graphs.
- Frank De Clerck: Constructions and characterizations of finite incidence structures and their adjacency graphs, with the emphasis on (semi)partial geometries, generalized quadrangles, and near polygons. Spreads of (semi)partial geometries. Distance regular graphs and their geometries. Projective and affine embedding of  $(\alpha, \beta)$ -geometries. Two-weight codes. Characterization of projections of polar spaces.
- Nikias De Feyter: Constructions and characterizations of full embeddings of  $(0, \alpha)$ -geometries and semipartial geometries in finite projective and affine spaces. Characterization of projections of polar spaces.
- Joris De Kaey: Characterizations of finite generalized polygons containing a subpolygon with large stabilizer group.
- Tom De Medts: An algebraic study of (spherical) buildings, including Moufang sets, and links with algebraic groups and non-associative algebras (including Jordan algebras).

- Stefaan De Winter: Characterization and classification of SPG-systems, construction and characterization of SPG-reguli and semipartial geometries. Semi-pseudo-ovals. Regular group actions on generalized quadrangles and partial geometries.
- An De Wispelaere: Ovals, spread, distance-2-ovals and distance-2-spreads in finite generalized hexagons; Holz design in generalized hexagons; unital; one-point extensions of generalized hexagons and octagons.
- Patrick Govaerts: Blocking sets, (partial) ovals, covers, (partial) spreads, Cameron-Liebler line classes, Latin squares.
- Nele Haelvoet: Properties and projective embeddings of geometries with few points on every line, and their connection with graphs, polarities and automorphism groups.
- Fabienne Haot: Characterization and classification of generalized polygons using properties of their automorphism groups.
- Elisabeth Kuijken: Regular two-graphs, incidence structures ((semi)partial geometries, generalised polygons), codes, and their connections.
- Deirdre Luyckx: Partial  $m$ -systems of finite classical polar spaces: examples, constructions, characterizations, bounds on their sizes. Geometrical interpretation of difference sets. Spreads of the split Cayley hexagon.
- Alan Offer: Finite generalized hexagons, finite generalized quadrangles, and (translation) spreads and (translation) ovals in them.
- Roland Puystjens: Generalized invertibility.
- Leo Storme: Study of substructures in finite projective spaces. The research was focussed on: Minihypers in  $PG(N, q)$ ; Multiple blocking sets in  $PG(2, q)$ ; Multiple  $k$ -blocking sets in  $PG(N, q)$ ; Caps in finite projective spaces; Blocking sets and ovals of classical polar spaces and of generalized quadrangles; Cameron-Liebler line classes.
- Joseph A. Thas: Generalized quadrangles of order  $(s, s^2)$ . Subquadrangles of generalized quadrangles. Translation generalized quadrangles. Moufang conditions for finite generalized quadrangles. Ovals and spreads of generalized quadrangles and generalized hexagons. Embeddings of generalized polygons. Arcs and caps in  $PG(n, q)$ . Partial  $m$ -systems and  $m$ -systems of polar spaces. Constructions of (semi)partial geometries.  $SPG$ -reguli and  $SPG$ -systems. Characterizations of Veronese varieties and their projections.
- Koen Thas: Automorphisms and characterizations of generalized quadrangles. Combinatorial structures in generalized quadrangles and their generalizations, such as complete  $(st - t/s)$ -arcs in generalized quadrangles of order  $(s, t)$ , and (translation) ovals and spreads in generalized quadrangles. Translation generalized quadrangles — interrelation with the translation dual, classification, semifield flocks, translation generalized ovals, good generalized ovals in even characteristic, 2-transitive generalized ovals. Elation generalized quadrangles — the completeness problems for elation groups. Lenz-Barlotti classifications for finite generalized quadrangles. Moufang conditions for generalized quadrangles. Characterizations of the classical and dual classical generalized quadrangles. Number of points on hypersurfaces. Finite flag-transitive projective planes, power residue difference sets, Gauss sums and Fermat surfaces.

- Cristina Tonesi: Geometries with incidence number 2: constructions of new models, characterizations, classification and automorphisms, connection with two-weight codes. Distance regular geometries. Moufang 3-nets.
- Pieter Vandecasteele: Classification and characterization of near polygons.
- Hendrik Van Maldeghem: Moufang sets, automorphisms of generalized quadrangles, finite flag transitive generalized polygons, transitive and geometric homogeneous geometries with three points per line and three lines per point, partial linear spaces from generalized hexagons, extensions of generalized polygons, relaxing the Moufang condition for Moufang polygons, intransitive flipflop geometries and amalgams, Moufang conditions for  $(0, 2)$ -geometries, grumbling embeddings of classical polygons, 2-character sets in projective 5-space.

**3.1.6 Universiteit van Tilburg,  
Faculty of Economics and Business Administration,  
Econometrics and Operations Research Group**

**Research activities:**

- Edwin van Dam:  
Latin hypercube designs; spectral characterizations of distance-regular graphs.
- René Peeters:  
Building a solver for set partitioning problems; chromatic number and ranks of matrices of graphs.
- Willem Haemers:  
Combinatorial designs, distance-regular graphs; spectral characterizations of graphs.

**3.2 Coding Theory, Information Theory and Cryptology**

**3.2.1 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,  
Nationaal Bureau voor Verbindingsbeveiliging, Den Haag**

- M.J.M.M. van Asperdt: Block- and stream ciphers and their implementation.
- B. Botma: Software Security and weaknesses.
- P.A.H. Bours: Public key systems and their implementation.
- R.W.M.G. Doijen: Key management architecture and its implementation.
- L.P. van Drimmelen: Software Security and weaknesses.
- J.W.L. Drossaers: Software Security and weaknesses.
- E. van der Laan: Software Security and weaknesses.
- S. Oudkerk: Network security and vulnerabilities.
- C.L.M. van Pul: Key management architecture and its implementation.
- K. van der Raad: Software Security and weaknesses.
- G. Roelofsen: Block- and stream ciphers and their implementation.

- G. Schmitz: Public key systems and their implementation.
- J.M.J.B. van Zanten: Network security and vulnerabilities.

**3.2.2 Technische Universiteit Eindhoven,  
Department of Mathematics and Computer Science,  
Discrete Mathematics Group**

**Coding Theory**

Closed formulas for the error-locator polynomial of binary cyclic codes are derived. A book on algebraic geometry codes is in the ongoing process of being written.

**Cryptography**

Work on Differential Power Analysis (DPA) attacks had been done in the past in several thesis projects. The Hamming weight model is a way to model the power consumption of a smart card or similar computing device. For the Hamming weight model we started to investigate the expected size and variance in the height of the peaks of the differential trace for 2nd-order DPA. Note that many implementations are routinely protected against 1st-order DPA these days, hence it's important to have a good understanding of 2nd-order DPA.

Several topics in quantum cryptography were studied. One line of work concerns a variant of the well-known 1984 Bennett-Brassard protocol for quantum key distribution. The variant was proposed by Gottesman and Preskill in 2000 and uses squeezed states instead of single photons. The security of the GP00 protocol is analyzed by adapting the approach proposed by Christandl, Renner and Ekert for analyzing the BB84 protocol. Another line of work concerns the information-theoretical analysis of various quantum secret sharing schemes, ranging from basic threshold schemes to schemes for arbitrary monotone access structures. The security of various constructions is proved. Also, the connections between quantum threshold schemes and quantum MDS codes are investigated.

The work on verifiable secret sharing schemes in the unconditional setting was continued. The conditional gate has been introduced as a building block for secure computation, either in the two-party case or multi-party case. In this approach to secure computation a threshold homomorphic cryptosystem is assumed, and for the conditional gate one can use a simple ElGamal based cryptosystem. Applications of the conditional gate have been considered, specifically in the area of profile matching and matching of encrypted biometric templates.

A generalization of the basic Pollard lambda algorithm is revisited, which is actually applicable in protocols for electronic voting. The goal is to limit the storage for the algorithm as much as possible, while computing the result in square root time (Pollard lambda also uses square root time). Work has been done on searching in structured but encrypted databases. Here, the client and a server share the exact contents of the database, such that the client only needs to store a seed value to reconstruct its share. Specifically, the problem of searching in text is considered. A study of verifiable MIXes was performed. Verifiable MIXes can be used as a building block in election schemes, and several protocols are studied, some of which achieve linear complexity (linear in the number of ciphertexts being mixed). Aspects of the robustness and security of optical PUFs (Physically Unclonable Functions) have been studied by investigating

how the resulting speckle patterns can be handled.

An efficient extension of Wiener's small private key attack on RSA has been developed, that works when a part of the private key is already known to the attacker. It illustrates the link between continued fractions and lattices, since the attacks of Wiener and Verheul/van Tilborg using continued fraction methods appear as special cases of the new attack that uses a 2-dimensional lattice. Moreover, other new partial key exposure attacks on RSA have been found using Coppersmith techniques. In essence, it has been shown that when either the private exponent  $d$  or the public exponent  $e$  of RSA is chosen to be significantly smaller than the modulus  $N$ , then only a fraction of  $d$  suffices to expose the private information. These attacks therefore expose new sections of the RSA key space that are vulnerable when the private key is partially known.

Research into the problem of secure 2-party computation is started; it focuses in particular on fairness. Yao's garbled circuit approach is studied, which is used in a paper by Pinkas (Eurocrypt 2003). Improvements and simplifications of the protocols by Pinkas are made. The results for the garbled circuit approach will be compared with secure 2-party computation based on a gate-by-gate approach (which in turn is based either on threshold homomorphic cryptosystems or on oblivious transfer combined with VSS).

A common feature of almost all cryptographic schemes is that they use randomness. One of the most fundamental issues in modern cryptology is randomness. Randomness is used for probabilistic encryption and digital signature algorithms; nonces and session keys in cryptographic protocols must be random. However, in practice true randomness is hard (if not impossible) to achieve. A possible solution to this problem is proposed by the theory of cryptographically secure pseudorandom generators. A thorough research has been done to analyze known constructions for the pseudorandom generators.

Quite some effort has been put in an Encyclopedia of Cryptography and Security that is scheduled to appear in 2005. The Advisory Board consists of 20 renowned researchers in the field. Pairing-based cryptography has been studied, providing some detailed proofs that seem to be absent in the literature, as well as an expository implementation of pairing computation. Also applications of pairing-based cryptography was studied, resulting in a practical comparison with conventional PKI.

Algebraic attacks were studied from a Gröbner basis perspective. The relation between F4, F5 and XL on the one hand and Gröbner Basis methods on the other hand has been clarified and made explicit, showing that XL can be seen as a cumbersome way to compute Gröbner bases. It is shown how one can use these methods to distinguish between algebraic systems, like HFE, that are easier to solve than random systems.

#### Miscellaneous

An overview has been written of all the work presented at the WIC Symposia on Information Theory during the last 25 years. Organizing and editing the Proceedings of the 25-th Symposium on Information Theory in the Benelux, April 2004 at Kerkrade.

**3.2.3 Technische Universiteit Eindhoven,  
Department of Electrical Engineering,  
Information and Communication Systems Group**

**Overview of academic results 2004**

Various information-theoretic results were obtained.

- A journal paper on embedding in grayscale signals was accepted. A conference-paper on reversible embedding was accepted and appeared in a DIMACS series (AMS) book.
- Semantic source coding is a special (zero-rate) case of reversible embedding, in which the code words are constrained to be meaningful. In two lectures about semantic noiseless source coding (one invited) we presented the optimal trade-off between compaction rate and distortion between source sequence and codeword. Results obtained by former student D. Maas on optimal test-channels for reversible embedding also apply here.
- Together with researchers from the University of Toronto a joint paper was produced on the Blahut-Arimoto algorithm which combines our results on computation of the Wyner-Ziv function and their methods for computing Gelfand-Pinsker capacities.
- In the Mode-Group Diversity Multiplexing (MGDM) project, together with the ECO group, three conference papers were produced that explore proper models of optical channels and receivers, emphasizing commonalities with communications at radio frequencies.
- Together with Albert Guillen and Giuseppe Caire (Eurecom, France), novel techniques were devised which significantly simplify, with no loss of accuracy, previous methods to estimate the error probability of bit-interleaved coded modulation. This work was described in two conference papers. A journal manuscript has been submitted.
- Joint work with M. Rovina (ESA) led to a new fast stopping rule for turbo-like iterative decoders, presented at IWT 2004 (Brazil). In addition, a paper, accepted for publication in February 2005 was submitted, with M. Lamarca (UPC, Spain), on Soft-Decision Reed-Solomon decoders.

A chapter on source coding was contributed to a book on "Information Theory in the Benelux: An overview of WIC symposia 1980-2004".

In recognition of his pioneering contributions to the area of network information theory, F. Willems was elected IEEE Fellow.

**Programme development**

Research on Universal modeling and compression will be developed in two directions. We shall consider special compression topics such as coding for non-stationary sources, compression of data with large alphabets, and random-access decompression. Research here will be done in collaboration with Dr. Shamir, University of Utah. We shall consider the modeling and prediction aspects of universal coding together with Dr. de Vries, GN ReSound. In particular the relation between the minimum description length principle, Gaussian mixtures, and Bayesian networks will be considered here.

Our information-theoretic work will continue to address semantic coding theory, and will also focus on permuting channels. Moreover, past work on biometric

schemes will be extended. Specifically, the relation between quantization index modulation and template protection will be studied in order to design methods that are more reliable than the current ones.

Work on mode-group diversity multiplexing (MGDM) will focus on the design, realization and validation of an experimental prototype system. To this end the project will be reinforced with an MTD student from DTI.

### **3.2.4 TNO Information and Communication Technology, Delft**

Research activities

Telecommunication security:

- Security of Telecommunication Services: m-commerce security, i-mode security, innovative PKI based services, Digital Rights Management, VoIP security, IP Multimedia Sub-system security.
- Security of Wireless Networks: 2G, 3G and 4G networks, SIM/USIM.
- Security of Fixed Telco Networks: Payphone security, ATM security, IN security, OSA/Parlay security.
- Fraud Management: fraud detection in fixed and cellular telco networks.
- Lawful interception of telecommunication services.
- IT and network security.
- Access control, RBAC, IDS, DDoS detection and prevention, IPsec, TLS/SSL, Web Service Security, WLAN security.
- Information Security Management.
- ISO/IEC 17799, BS 7799-2:2002, security assessments, risk analysis and audits.

### **3.2.5 Universiteit Gent, Belgium, Department of Pure Mathematics and Computer Algebra, Research Group Incidence Geometry**

- An De Wispelaere: Projective two-weight codes; codes from generalized hexagons.
- Patrick Govaerts: Linear codes meeting the Griesmer bound.
- Leo Storme: Linear codes meeting the Griesmer bound; Codes over rings; Reversible logic gates.

### **3.2.6 Université Catholique de Louvain, Belgium, UCL Crypto Group**

Research subjects:

Smart cards, crypto-processors, cryptology, security, zero-knowledge, elliptic curves, cryptographic watermarking, trusted third party, secure remote loading, Pay-TV, electronic purse, internet security, secure timestamping, software and hardware implementations, faulty cryptographic computations.

### 3.3 Combinatorial Optimization, Combinatorial Algorithms and Graph Theory

#### 3.3.1 Centrum voor Wiskunde en Informatica, Amsterdam, Group Networks and Logic - Optimization and Programming

##### Highlights

- June 23-25, the 8th International Workshop on High Performance Optimization Techniques (HPOPT 2004) took place at CWI. It was chaired by M. Laurent and part of her NWO-Vidi project Semidefinite Programming and Combinatorial Optimization.
- W.J. van Hoeve received the Best Student Paper Award at the Tenth International Conference on Principles and Practice of Constraint Programming (CP 2004), September 27-October 1, Toronto, for his paper: A Hyper-arc consistency algorithm for the soft alldifferent constraint.
- A. Schrijver received the Lanchester Prize of the Operations Research Society of America, for his book: *Combinatorial Optimization—Polyhedra and Efficiency*, for the best publication in Operations Research in 2003.
- J.K. Lenstra received an INFORMS Fellow Award at the INFORMS Annual Meeting in Denver.

##### Research results

*Semidefinite Programming and Combinatorial Optimization:* M. Laurent continued her research on the optimization of polynomials and semidefinite programming. Together with E. de Klerk and P. Parrilo she gave a polynomial time approximation scheme for the minimization of a polynomial of fixed degree over the standard simplex. Together with D. Jibeteau, she developed a method for constructing tight approximations (with certificates) for the global infimum of a polynomial. Together with N. Gvozdenović, she partially proved a conjecture of de Klerk and Pasechnik on the number of iterations needed for finding the stability number of graphs in a hierarchy of semidefinite bounds based on sums of squares of polynomials.

*Bounds from algebra and semi-definite programming:* A. Schrijver found new bounds on the size of binary codes, based on block-diagonalizing the Terwilliger algebra and on semidefinite programming. With D. Gijswijt and H. Tanaka, this was extended to nonbinary codes. A. Schrijver extended a method of De Klerk et al., based on matrix algebra and semidefinite programming, to obtain improved lower bounds on the crossing number of complete bipartite graphs. With C. Luz, A. Schrijver found a new characterization of Lovász's  $\vartheta$  bound on the stable set number of graphs.

*Routing and disjoint paths:* É. Colin de Verdière and A. Schrijver worked on the following problem: given a weighted planar undirected graph and  $k$  pairs of terminals, compute the shortest set of  $k$  vertex-disjoint paths connecting these pairs. While this problem is NP-hard in general, they prove that it is solvable in strongly polynomial time if there are two faces each meeting each of the terminal pairs. L. Stougie and R. Sitters (TUE) simplified the proof of competitiveness of the general two-server problem by deriving a general competitiveness characterization for metrical service systems. This also improved the competitive ratio considerably. L. Stougie, C. Hurkens (TUE) and J. Keijsper (TUE) studied symmetric virtual private networks, where one needs to buy bandwidth on the

links to facilitate communication between users in the network. The conjecture is that there always is an cheapest solution that forms a tree. This was known for circuit networks. Stougie et al. extended it to a larger class. L. Stougie, M. Skutella (Univ. Dortmund), L. Becchetti and A. Marchetti Spaccamela (both La Sapienza, Rome) derived complexity and approximation results for networks of sensors that have to send data with a maximal allowed delay to a central computer with few broadcasts, to save battery energy.

*Stochastic programming:* L. Stougie, W. Klein Haneveld and M. van der Vlerk (both RUG) studied convex approximations in stochastic integer simple recourse problems. A full characterization of distributions that lead to convex objective functions has been derived and approximation based on this class of functions has been studied, yielding bounds on the absolute approximation error.

*Facility location:* L. Stougie, J. van den Broek (TUE) and A. Tomasgard (NTNU, Trondheim), studied location of slaughter houses for Norwegian Meat Cooperation where the facility costs obeyed economics of scale. A branch and bound approach using Lagrangian relaxation for lower bounds reached solutions provably close to optimal. Together with A. Tomasgard (NTNU, Trondheim) and P. Schülz (NTNU, Trondheim) the work was extended to the more realistic stochastic setting.

*Structure and representability of networks, matrices and matroids:* In their long-term project on matroid structure and matroid representability, A. Gerards, J. Geelen (Univ. Waterloo, Ont.) and G. Whittle (Victoria Univ., Wellington, New Zealand) determined the structure of matroids that are represented over a finite field and have neither the cycle matroid nor the cocycle matroid of a large apexed square grid as a minor. They also described when a triple of elements in a representable matroid is not contained in a circuit. It turns out that this is essentially only the case if the matroid is a so-called Dowling matroid, which is a graph-like matroid, and the three elements are so-called "joints" of these Dowling matroids. It is the first explicit evidence for the team's believe that Dowling matroids are the main building blocks for the structure of matroids that are represented over a finite field.

*Packing odd circuits:* A. Gerards and M. Conforti revisited a class of graphs where a maximum packing of odd circuits can be found in polynomial time and worked out algorithms to find these packings and to recognize the graphs.

*Integer Programming Techniques:* K. Aardal has together with A.K. Lenstra developed an algorithm for proving feasibility of a class of 0-1 integer programming problems using a reduction to the closest vector problem. This algorithm is under implementation. She also showed, together with J. de Loera and L. Wolsey, how to compute the Chvatal-Gomory closure of a rational polytope in polynomial for fixed dimension via Barvinok's rational functions. This is part of an ongoing larger research project.

*Algorithmic and Combinatorial Methods for Molecular Biology:* Together with T. Boekhout (CBS KNAW), E. Kuramae (BBS KNAW), V. Robert (CBS KNAW), R. Cilibrasi (CWI), J. Tromp (INS4) and P. Vitanyi (INS4), L. Stougie worked on constructing phylogenetic trees for fungi species.

*Design and analysis of algorithms for railway network optimization:* In cooperation with P.J. Fioole and L.G. Kroon of NS Reizigers, G. Maróti and A.

Schrijver, designed, tested and implemented algorithms for the optimal circulation of railway rolling stock. At one hand, this concerns the nation-wide planning (in particular the ‘Noord-Oost’: the network connecting Amsterdam, The Hague, and Rotterdam at one side, and Enschede, Leeuwarden, en Groningen at the other side), at the other hand the problem of planning and optimizing the shunting and maintenance of trains at railway yards. Main complicating issue is that trains of different characteristics can be combined to one train or can be stored on the same track. G. Maróti also worked on maintenance routing. He simplified earlier derived models, proved complexity results and carried out computational experiments on real-world instances.

*Methods for integer and constraint programming:* W.J. van Hoeve considered the propagation of the all-different condition in constraint programming, and how branching decisions in solving integer programming can be postponed. This is very useful in decision support systems in which conditions on exclusive assignments or selections are posed. This can also be framed into integer programming framework. K. Aardal studied various lattice basis reduction algorithms that are used as auxiliary algorithms when solving integer feasibility and optimization problems. These algorithms are based on the idea of branching on lattice hyperplanes, and their running time is polynomial in fixed dimension. Among the algorithms considered are binary search, a linear algorithm for a fixed number of constraints, and a randomized algorithm for a varying number of constraints.

### **3.3.2 Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, Combinatorial Optimization Group**

#### **Graphs and matroids**

In their long-term project on matroid structure and matroid representability, A. Gerards, J. Geelen (University of Waterloo, Ontario) and G. Whittle (Victoria University, Wellington, New Zealand) determined the structure of matroids that are represented over a finite field and have neither the cycle matroid nor the cocycle matroid of a large apexed square grid as a minor. They also described when a triple of elements in a representable matroid is not contained in a circuit. It turns out that this is essentially only the case if the matroid is a so-called Dowling matroid, which is a graph-like matroid, and the three elements are so-called ”joints” of these Dowling matroids. It is the first explicit evidence for the team’s believe that Dowling matroids are the main building blocks for the structure of matroids that are represented over a finite field.

A. Gerards and M. Conforti revisited a class of graphs where a maximum packing of odd circuits can be found in polynomial time and worked out algorithms to find these packings and to recognize the graphs.

H. van der Holst and R. Pendavingh investigated the embeddability in Euclidean  $d$ -space of certain cell complexes related to graphs. They coined a topological graph invariant which generalizes both planarity and linkless embeddability of graphs, and proved a general bound on the new invariant in terms of a geometrical graph invariant of van der Holst, Laurent and Schrijver.

#### **Polyhedral combinatorics**

Under supervision of L. Stougie, P. Korteweg started as a PhD-student investigating diameters of network polyhedra. He made a first survey of all known results in the literature.

### **New models and methods for routing problems**

R.A. Sitters and L. Stougie simplified the proof of competitiveness of the general two-server problem, through deriving a general competitiveness characterization for metrical service systems. At the same time they improved the competitive ratio considerably.

The project on routing problems supervised by L. Stougie culminated in a Cum Laude PhD thesis of R.A. Sitters.

### **New models and methods for scheduling problems**

Under supervision of C.A.J. Hurkens, J.J.J. van den Broek started as a PhD student, studying scheduling problems with material constraints. These concern the scheduling of trains, as well as the scheduling of manufacturing processes with spatial restrictions.

J.J.J. van den Broek together with C.A.J. Hurkens and L.G. Kroon (Erasmus University of Rotterdam/ NS Reizigers) worked on a capacity test for railway related shunting movements. The model has been extended and a start is made with the implementation of the developed tool in the actual planning proces of the Dutch railways.

### **Stochastic programming**

Together with W. Klein Haneveld (Groningen University) and M.H. van der Vlerk (Groningen University), L. Stougie finished a paper on convex approximations in stochastic integer simple recourse problems. A full characterization of distributions that lead to convex objective functions has been derived and approximation based on this class of functions has been studied, yielding bounds on the absolute approximation error.

Together with M.H. van der Vlerk (Groningen University) L. Stougie finished a major revision of a chapter on approximation algorithms in stochastic programming for a handbook on approximation algorithms.

Together with S. Leonardi (La Sapienza University Rome) and C. Swami (Caltech, Los Angeles), L. Stougie initiated work on stochastic scheduling problems, in which processing resources are to be bought before a realization of the job parameters is known. In a second stage a recourse action may provide (at higher cost) additional resources.

### **Mathematics and biology**

Research on the interface of mathematics and biology has been continued. Together with T. Boekhout (CBS KNAW), E. Kuramae (BBS KNAW), V. Robert (CBS KNAW), R. Cilibrasi (CWI), J. Tromp (CWI) and P. Vitanyi (CWI), L. Stougie worked on constructing phylogenetic trees for fungi species. A common project proposal has been prepared.

Within the context of BRICKS research project AFM2.1 Steven Kelk has been acquired as a Post-Doc. Together with S. Kelk (CWI), R. Celibrasi (CWI) and J. Tromp (CWI), C.A.J. Hurkens, J.C.M. Keijsper, G.J. Woeginger, and L. Stougie started a Computational Molecular Biology seminar, studying the books in that field. Some first research questions considering some haplotyping problems are being investigated.

### **Network optimization problems**

C.A.J. Hurkens, J.C.M. Keijsper, and L. Stougie worked on a conjecture concerning so-called symmetric virtual private networks. The problem is to route possible traffic (communication) between the users in such networks, and to buy bandwidth on the links of the network to accommodate this traffic, in such a way that the total cost for buying bandwidth is minimal. The conjecture is that a tree in the network always gives an optimal solution. They extended the class of networks beyond circuit networks for which the conjecture can be proved.

Together with L. Becchetti, A. Marchetti Spaccamela and A. Vitaletti (La Sapienza University Rome) and M. Skutella (University Dortmund), L. Stougie initiated research on sensor networks. A network of sensors have to sense data and send them to a central computer, using as few as possible broadcasts to save battery energy, but respecting a maximal allowed delay. First complexity and approximation results have been obtained.

### **Facility location problems**

Together with J.J.J. van den Broek (TUE) and A. Tomasgard (NTNU, Trondheim), L. Stougie studied a facility location problem from Norwegian Meat Cooperation. It concerned the location of slaughter houses and had the peculiar property that the facility costs obeyed economics of scale. A branch and bound approach using Lagrangian relaxation for lower bounds reached solutions provably close to optimal. Together with A. Tomasgard (NTNU, Trondheim) and Peter Schülz (NTNU, Trondheim) the work was extended to the more realistic stochastic setting.

External research contacts:

- M.E. Dyer (Leeds University, UK)
- S. Dye (University of Canterbury, New Zealand)
- A. Tomasgard (NTUT Trondheim, Norway)
- L. Becchetti (La Sapienza, Rome, Italy)
- S. Leonardi (La Sapienza, Rome, Italy)
- A. Marchetti Spaccamela (La Sapienza, Rome, Italy)
- S. Krumke (University Kaiserslautern, Germany)
- M. Skutella (University Dortmund, Germany)
- M. Goemans (MIT, Cambridge MA, USA)
- N. Megow (TU Berlin, Germany)
- L. Kroon (NS Reizigers/ EUR Rotterdam)
- J. Sgall (Chzech Academy of Sciences, Prague, Chzechia)
- S. Dye (University of Canterbury, Christchurch, New Zealand)
- T. Boekhout (Centraal Bureau voor Schimmelcultures, KNAW, Utrecht)
- E. Kuramae (Centraal Bureau voor Schimmelcultures, KNAW, Utrecht)
- V. Robert (Centraal Bureau voor Schimmelcultures, KNAW, Utrecht)

- X. Lu (University of East China, Shanghai, China)
- K.M.J. De Bontridder (Siemens, Eindhoven)
- A.P.A. Vestjens (CQM, Eindhoven)

### 3.3.3 Université Libre de Bruxelles, Belgium, Département de Mathématique

- Group Graphes et Optimisation Mathématique:
  - Sophie Dewez: Bilinear bi-level programming.
  - Gilles Fasbender: Combinatorial optimization, cutting stock, column generation.
  - Luigi De Giovanni: Combinatorial optimization, network design, delay management.
  - Geraldine Heilporn: Combinatorial optimization, bilinear bi-level programming, delay management.
  - David Huygens: Combinatorial optimization, network design problems.
  - Martine Labbé: Combinatorial optimization, graphs, location and network design.
  - Hadrien Mélot: Graph theory, computer assisted / automated conjectures.
  - Aykut Özsoy: Combinatorial and network optimization.
  - Mathieu Van Vyve: Mixed-integer programming, production planning, polyhedral combinatorics.
- Service de mathématiques et d'informatique générales :
  - Jean-Paul Doignon: Facets of the linear ordering polytope and a weighted generalization of stability-critical graphs (joint work with Samuel Fiorini and Gwenaël Joret). Transposition distance between two permutations (joint work with Anthony Labarre). Turán Theorem for connected graphs (joint work with Martine Labbé and her team).
  - Samuel Fiorini: Minmax relations for covering problems based on 2-packings. Approximability and inapproximability of certain scheduling problems. Minimum entropy colorings in probabilistic graphs.
  - Gwenaël Joret: Facets of the linear ordering polytope and a weighted generalization of stability-critical graphs (joint work with Jean-Paul Doignon and Samuel Fiorini). Minimum entropy colorings in probabilistic graphs (joint work with Jean Cardinal and Samuel Fiorini)
  - Anthony Labarre: Transposition distance between two permutations (joint work with Jean-Paul Doignon).

### 3.3.4 Universiteit Gent, Belgium, Dept. of Applied Mathematics and Computer Science, Group Combinatorial Algorithms and Algorithmic Graph Theory

- Gunnar Brinkmann: Classification and filtering of Yutsis graphs. Fullerene growth by patch replacement. Generation of restricted classes of graphs.

- Jan Degraer: Algorithms for exhaustive generation of association schemes with given parameters.
- Veerle Fack: Classification and reduction of Yutsis graphs.
- Dries Van Dyck: Classification and reduction of Yutsis graphs.

**3.3.5 Universiteit Twente,  
Faculty of Mathematical Sciences,  
Group Discrete Mathematics and Mathematical Programming**

**Approximation algorithms**

W. Kern and G. Woeginger investigated the approximability of combinatorial minimum weight product problems, like, e.g., computing an  $s - t$  path  $P$  in a graph, such that the product  $a(P)b(P)$  of two different edge weights is (approximately) minimized.

T. Nieberg, J.L. Hurink and W. Kern consider graph problems in unit disk graphs where no geometric representation of the vertices is given. They develop robust polynomial-time approximation schemes for the maximum independent set problem and for the minimum dominating set problem.

**Scheduling theory**

J.L. Hurink and S. Knust investigate a job-shop scheduling problem where the jobs have to be transported between the machines by a single transport robot.

M.J.R. Ebben, M.C. van der Heijden, J.L. Hurink and J.M.J. Schutten consider transportation problems in which the finite capacity of resources has to be taken into account. They present a flexible modeling methodology which allows to construct, evaluate, and improve feasible solutions.

P. Brucker, S. Heitmann, J.L. Hurink, and T. Nieberg investigate an extension of the classical flow-shop problem, where between each two consecutive machines a buffer of limited capacity is given.

**High school timetabling**

G.F. Post and H.W.A. Ruizenaar are working on the construction of Dutch high school (year) rosters. The first step usually consists of constructing the so-called clusterscheme. A branch & bound algorithm has been constructed to enumerate all possibilities that occupy at most a (user given) maximum number of timeslots. For a medium size high school, solutions are found within a few minutes. The second step is assigning the lessons to timeslots. A 2-phase approach for this is used. First the lessons are assigned to one of the 10 day parts of the week. This is done by an adaptive heuristic ordering. The second phase assigns the lessons (per day part) to timeslots. Finally a Tabu search further improves the result. The time needed for the second part, also is measured in minutes (5 to 10 minutes).

**Cycles in graphs**

A.N.M. Salman, E.T. Baskoro and H.J. Broersma studied hamiltonicity and smallest 2-connected spanning subgraphs of several classes of grid graphs. They revised and completed a series of papers on this topic which will also be part of Salman's PhD thesis. An update on toughness on graphs was written by D. Bauer, H.J. Broersma and E. Schmeichel. An extended survey will appear in Graphs and Combinatorics. The new concept of  $f$ -connectivity and its re-

lation to cyclic properties of graphs was studied in a joint paper of S. Brandt, H.J. Broersma, R. Diestel and M. Kriesell. This paper has recently been accepted for publication in *Combinatorica*.

### **Graph colorings**

H.J. Broersma, F.V. Fomin and G.J. Woeginger investigated a number of graph coloring problems that result from frequency assignment problems in radio networks. A paper with a full classification of the computational complexity of planar graph colorings avoiding monochromatic subgraphs has been accepted for publication in *Algorithmica*. They derived algorithmical and combinatorial results on so-called backbone colorings. A paper has been submitted to *SIAM J. on Discrete Mathematics*. Similar results were obtained in joint work with Fujisawa and Yoshimoto, and with D. Paulusma and A.N.M. Salman. This has been submitted to *Graphs and Combinatorics*. Structural and distance 2-coloring results on planar graphs were obtained in joint work of O.V. Borodin, H.J. Broersma, A. Glebov and J. van den Heuvel. A fourth paper on these topics is on its way. In a series of papers with E. Baskoro and Surahmat and A.N.M. Salman, H.J. Broersma established ramsey type results for different combinations of graph classes. J. Fiala and D. Paulusma studied locally surjective homomorphisms. They classified the corresponding decision problem and showed further corollaries for related problems. A. Levin, D. Paulusma and G.J. Woeginger studied the computational complexity of graph contractions.

### **Semi-infinite optimization and related topics.**

Georg Still studied different relaxation methods for solving semi-infinite problems with variable index sets and analyzed the convergence behavior of the approaches. Furthermore the connection between semi-infinite programming and Chebyshev approximation was investigated from the viewpoint of reverse approximation.

### **Applications**

H.J. Broersma and J.L. Hurink worked in different combinations with colleagues from the Department of Computer Science on applications. Control systems are developed, which adapt at run-time to the dynamic external environment. The goal is to operate with minimized use of resources and energy consumption, while satisfying an adequate quality of service. Another area is related to the design of heterogeneous reconfigurable systems on chip. Here data flow graphs have to be mapped to an architecture graph of a reconfigurable tile.

T. Nieberg and J.L. Hurink worked on optimizations problems occurring for mobile ad-hoc sensor networks. They deal with distributed clustering schemes and topology control.

### **Set games**

A. Bumb and C. Hoede have introduced the concept of standard set game corresponding to a normal cooperative game. They used standard set games to give a natural splitting of a cooperative game into a reward game and a fine game. They also gave two new families of solidarity values.

### **Knowledge graphs**

C. Hoede investigated the relationship between knowledge graph theory and the structuralistic linguistic theory of Ebeling. Both theories turned out to be rather similar.

**Computational and cooperative game theory**

U. Faigle, W. Kern and J. Kuipers analyzed the computational complexity of the kernel, a standard solution concept for cooperative games.

T.S.H. Driessen completed joint research with Holger Meinhardt (Karlsruhe, Germany) on the convexity property for cooperative games arising from some economic situation, like oligopoly or common pool situations. Further, Hamiache's recent axiomatic characterization for the Shapley value in terms of the associated consistency has been extended to the class of efficient, symmetric, and linear values, of which the Shapley value is the most important representative. It concerns a combinatorial proof.

## 4 Publications in 2004

### 4.1 Books

- A.M. Cohen, *Distance-transitive graphs*, In: L.W. Beineke, R.J. Wilson and P.J. Cameron (eds.), *Topics in Algebraic Graph Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 102, 2004, 222–249.
- K.A.S. Immink, *Codes for mass data storage systems*, Second fully revised edition, Shannon Foundation Publishers, Eindhoven, The Netherlands, ISBN 90-74249-27-2, November 2004.
- K.A.S. Immink, *Codes for mass data storage systems* (in Chinese), Science Press, Beijing, China, 2004, ISBN 7-03-013379-X.
- K.A.S. Immink, *Coding and signal processing for magnetic recording systems*, In: E.M. Kurtas and B. Vasic (eds.), Section IV, page 17-1, CRC Press, Series: Computer Engineering Volume: 2, ISBN 08-49315-24-7, November 2004.
- K.A.S. Immink, L.M.G.M. Tolhuizen and J.H. Weber, *Channel coding*, Chapter 4 (pp. 89-116) in: R.L. Lagendijk, L.M.G.M. Tolhuizen and P.H.N. de With (eds.), *Information Theory in the Benelux: An overview of WIC symposia 1980-2003*, Werkgemeenschap voor Informatie- en Communicatietheorie (WIC), Enschede, May 2004, ISBN 90-71048-19-5.
- R.J. Stroeker and B.M.M. de Weger, *On integral zeroes of binary Krawtchouk polynomials*, In: N. Virchenko, I. Katchanovski, V. Haidey, R. Andrushkiw and R. Voronka (eds.), *Development of the mathematical ideas of Mykhailo Kravchuk (Krawchouk)*, Shevchenko Scientific Society, New York, USA, 2004, 623–633.
- K. Thas, *Symmetry in finite generalized quadrangles*, Monograph, *Frontiers in Mathematics* 1, Birkhäuser, 2004, ISBN: 3-7643-6158-1.
- T.J. Tjalkens and F.M.J. Willems, *Chapter 2: Source coding*, *Information Theory in the Benelux: An overview of WIC Symposia 1980-2003*, L.M.G.M. Tolhuizen and P.H.N. de With (eds.), Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, ISBN 90-71048-19-5, 2004, 41-60.

### 4.2 Research articles in refereed journals

- K.I. Aardal, *Comments on the paper: Attacking the market split problem with lattice point enumeration*, *Journal of Combinatorial Optimization*, 8, 2004, 147–149.
- K.I. Aardal and A.K. Lenstra, *Hard equality constrained integer knapsacks*, *Mathematics of Operations Research*, 29(3), 2004, 724–738.
- P. Abramenko and H. Van Maldeghem, *Maps between buildings that preserve a given Weyl distance*, *Indag. Mathem.*, 15, 2004, 305–319.
- I. Anderson, A.G van Asch and J.H. van Lint, *Discrete mathematics in the high school curriculum*, *ZDM*, 36, 1, 2004, 105–116.
- Claude Archer, *Direct sum decomposition of geometries based on maximal subgroups*, *Journal of Geometry*, 2004, 12–18.

- A.G. van Asch, *On the structure of the ring  $Z[\sqrt[3]{2}]$* , Annals of Pure and Applied Logic, 16(2), 2004, 243–251.
- R.M. Avanzi, M. Ciet and F. Sica, *Faster scalar multiplication on Koblitz curves combining point halving with the Frobenius endomorphism*, In: Feng Bao, R.H. Deng and J. Zhou (eds.), Public Key Cryptography (PKC 2004), Lecture Notes in Computer Science, vol. 2947, Springer-Verlag, 2004, 28–40.
- Y. Azar, L. Epstein, Y. Richter and G.J. Woeginger, *All-norm approximation algorithms*, Journal of Algorithms 52(2), 2004, 120–133.
- C.P.M.J. Baggen, A. Nowbakht-Irani and A.J. Han Vinck, *Communication and modulation*, Information theory in the Benelux, An Overview of WIC Symposia, 1980-2003, ISBN 90-71048-19-5.
- S.M. Ball, J. Bamberg, M. Lavrauw and T. Pentilla, *Symplectic spreads*, Designs, Codes and Cryptography, 32(1-3), 2004, 9–14.
- J. Barát, A. DelFra, S. Innamorati and L. Storme, *Minimal blocking sets in  $PG(2, 8)$  and maximal partial spreads in  $PG(3, 8)$* , Designs, Codes and Cryptography, 31, 2004, 15–26.
- J. Barát, Y. Edel, R. Hill and L. Storme, *On complete caps in the projective geometries over  $F_3$ . II: New improvements*, J. Combin. Math. and Combin. Computing, 49, 2004, 9–31.
- J. Barát and L. Storme, *Multiple blocking sets in  $PG(n, q)$ ,  $n \geq 3$* , Designs, Codes and Cryptography, 33, 2004, 5–21.
- W. Barret and H. van der Holst, *Graphs whose minimal ranks is two*, Electronic Journal of Linear Algebra, 11, 258–280.
- E.T. Baskoro, H.J. Broersma and S. Surahmat, *The Ramsey numbers of large cycles versus small wheels*, INTEGERS, 4, 2004.
- J.W.M. Bergmans and A. Nowbakht, *Design of optimum sync and detection patterns for frame synchronization*, Electronic Letters, 40, 16, 2004, 1000-1001.
- J. De Beule, A. Hoogewijs and L. Storme, *On the size of minimal blocking sets of  $Q(4, q)$ , for  $q = 5, 7$* , ACM SIGSAM Bulletin, 149, 2004, 67–85.
- J. De Beule and K. Metsch, *The smallest minimal blocking sets of  $Q(2n, q)$ ,  $q$  prime*, Journal of Combinatorial Theory, Series A, 106, 2004, 327–333.
- A. Blokhuis and A.E. Brouwer, *Small additive quaternary codes*, European Journal of Combinatorics, 25(2), 2004, 161–167.
- H.L. Bodlaender, H.J. Broersma, F.V. Fomin, A.V. Pyatkin and G.J. Woeginger, *Radio labeling with preassigned frequencies*, SIAM Journal on Optimization, 15(1), 2004, 1–16.
- P.S. Bonsma, *Sparsest cuts and concurrent flows in product graphs*, Discrete Applied Mathematics, 136, 2004, 173–182.
- A. Born and G.J. Woeginger, *Wie man ohne Ariadnes Hilfe aus einem Labyrinth herausfindet*, Wissenschaftliche Nachrichten 124, 2004, 23–26.

- H.J. Broersma, C.L. Li, X. Li and L. Xiong, *The Hamiltonian index of a graph and its branch-bonds*, Discrete Mathematics, 285(1-3), 2004, 279–288.
- H.J. Broersma, C.A. Rodger and A.N.M. Salman, *A continuation of spanning 2-connected subgraphs in truncated rectangular grid graphs*, Journal of Combinatorial Mathematics and Combinatorial Computing, 49, 2004, 177–186.
- M.R. Brown, M.C. O’Keefe and C. Tonesi, *Partial Flocks of non-singular Quadrics in  $PG(2r+1, q)$* , Journal of Algebraic Combinatorics, 20, 2004, 359–370.
- M.R. Brown and J.A. Thas, *Geometrical construction of the oval(s) associated with an  $\alpha$ -flock*, Adv. Geometry, 4, 2004, 9–17.
- M.R. Brown and J.A. Thas, *Subquadrangles of order  $s$  of generalized quadrangles of order  $(s, s^2)$ , Part I*, Journal of Combinatorial Theory A, 106, 2004, 15–32.
- M.R. Brown and J.A. Thas, *Subquadrangles of order  $s$  of generalized quadrangles of order  $(s, s^2)$ , Part II*, Journal of Combinatorial Theory A, 106, 2004, 33–48.
- T. Brueggemann and W. Kern, *An improved deterministic local search algorithm for 3-SAT*, Theoretical Computer Science, 329(1-3), 2004, 303–313.
- B. De Bruyn, *Decomposable near polygons*, Ann. Comb. 8, 2004, 251–267.
- B. De Bruyn, *Near polygons having a sub near polygon isomorphic to  $G_n$* , Bulletin of the Belgian Mathematical Society Simon Stevin, 11, 2004, 321–341.
- B. De Bruyn and P. Vandecasteele, *Near polygons with a nice chain of sub near polygons*, Journal of Combinatorial Theory Series A, 108, 2004, 297–311.
- Ph. Bulens, G. Meurice de Dormale and J.-J. Quisquater, *Efficient modular division implementation—ECC over  $GF(p)$  affine coordinates application*, In: J. Becker, M. Platzner and S. Vernalde (eds), The 14th International Conference on Field Programmable Logic and Applications (FPL 2004), Lecture Notes in Computer Science, Springer, September 2004, 231–240.
- Sebastien Canard, Berry Schoenmakers, Martijn Stam and Jacques Traore, *List signature schemes*, invited paper for special issue of Discrete Applied Mathematics, 2004.
- Claude Carlet, Hans Dobbertin and Gregor Leander, *Normal extensions of bent functions*, IEEE Transactions on Information Theory, November 2004.
- J. Cathalo, B. Libert and J.-J. Quisquater, *Cryptanalysis of a verifiably committed signature scheme based on GPS and RSA*, In: K. Zhang, Y. Zheng (eds.), Information Security Conference (ISC) 2004, Lecture Notes in Computer Science, vol. 3225, Springer, 2004, 52–60.
- Wende Chen, Yuan Luo and A.J. Han Vinck, *The determination of the chain good weight hierarchies with high dimension*, SIAM Journal on Discrete Mathematics, 17(2), 2004, ISSN 0895-4801, 196–209.

- Julie Christophe, Jean-Paul Doignon and Samuel Fiorini, *The Biorder Polytope*, Order 21, 2004, 61–82.
- B. Chevallier-Mames, M. Ciet and M. Joye, *Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity*, IEEE Transactions on Computers, 53(6), June 2004, 760–768.
- M. Ciet, M. Neve and E. Peeters, *XTR implementation on reconfigurable hardware*, Cryptographic hardware and embedded systems - CHES2004, Lecture Notes in Computer Science, Springer-Verlag ©IACR, 2004
- F. De Clerck and M. Delanote, *On  $(0, \alpha)$ -geometries and dual semipartial geometries fully embedded in affine space*, Designs, Codes and Cryptography, 32, 1-3, 2004, 103–110.
- F. De Clerck, J.A. Thas and S. De Winter, *A characterization of the semipartial geometries  $T_2^*(U)$  and  $T_2^*(B)$* , European Journal of Combinatorics, 25, 2004, 73–85.
- A.M. Cohen, X.S. Gao and N. Takayama, *Editorial special issue on international congress of mathematical software (ICMS 2002, Beijing)*, Journal of Symbolic Computation, 38(4), 1167–1168.
- A.M. Cohen, S.H. Murray and D.E. Taylor, *Computing in groups of Lie Type*, Mathematics of Computation, 73(247), 2004, 1477–1498.
- B. Cooperstein, H. Van Maldeghem and J.A. Thas, *Hermitian Veroneseans over finite fields*, Forum Math., 16, 2004, 365–381.
- F.G.M.T. Cuypers, *Extended near hexagons and line systems*, Advances in Geometry, 4(2), 2004, 181–214.
- F.G.M.T. Cuypers and A. Steinbach, *Near hexagons and triality*, Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry, 45(2), 2004, 569–580.
- E.R. van Dam and E. Spence, *Combinatorial designs with two singular values I. Uniform multiplicative designs*, Journal of Combinatorial Theory A, 107, 2004, 127–142.
- J.-P. Doignon and S. Fiorini, *The facets and the symmetries of the approval-voting polytope*, Journal of Combinatorial Theory, Series B, 92, 2004, 1–12.
- J.-P. Doignon, A. Pekeč and M. Regenwetter, *The repeated insertion model for rankings: Missing link between two subset choice models*, Psychometrika, 69, 2004, 33–54.
- M.J.R. Ebben, M.C. van der Heijden, J.L. Hurink and J.M.J. Schutten, *Modeling of capacitated transportation systems for integral scheduling*, OR Spectrum, 26 (2), 2004, 263–282.
- S. Elloumi, M. Labbé and Y. Pochet, *New formulation and resolution method for the  $p$ -center problem*, INFORMS Journal on Computing, 16, 2004, 84–94.
- P.L. Erdős, U. Faigle, W. Hochstaettler and W. Kern, *Note on the game chromatic index of trees*, Theoretical Computer Science, 303(3), 2004, 371–376.

- C. Feremans, M. Labbé and G. Laporte, *The generalized minimum spanning tree problem: Polyhedral analysis and branch-and-cut algorithm*, Networks, 43, 2004, 71–86.
- S. Ferret and L. Storme, *A classification result on weighted  $\{\delta(p^3+1), \delta; 3, p^3\}$ -minihypers*, Journal of Combinatorial Design, 12, 2004, 197–220.
- S. Ferret and L. Storme, *On the size of complete caps in  $PG(3, 2^h)$* , Finite Fields Applications, 10, 2004, 306–314.
- N. De Feyter, *Planar oval sets in Desarguesian planes of even order*, Designs, Codes and Cryptography, 32 (1-3), 2004, 111–119.
- S. Fiorini, *A short proof of a theorem of Falmagne*, Journal of Mathematical Psychology 48, 2004, 80–82.
- S. Fiorini and P. Fishburn, *Weak order polytopes*, Discrete Mathematics, 275, 2004, 111–127.
- F.V. Fomin, D. Kratsch and G.J. Woeginger, *Exact (exponential) algorithms for the dominating set problem*, In: Proceedings of the 30th Workshop on Graph-Theoretic Concepts in Computer Science (WG'2004), LNCS 3353, Springer Verlag, 2004, 245–256.
- B. Fortz and M. Labbé, *Two-connected networks with rings of bounded cardinality*, Computational Optimization and Applications, 27, 2004, 123–148.
- F.-W. Fu, A.J. Han Vinck, V. Wei and R. Yeung, *On the capacity of write-unidirectional memories with nonperiodic codes*, IEEE Transactions on Information Theory, April 2004, ISSN 0018-9448, 649–656.
- B. Fuchs, W. Hochstaettler and W. Kern, *Online matching on a line*, Theoretical Computer Science, 2004.
- M. Gailly and D. Leemans, *The residually weakly primitive geometries of  $PSL(3, q)$  with  $q < 8$* , Aequationes Math. 67, 2004, 195–196.
- P. Govaerts and L. Storme, *On Cameron-Liebler line classes*, Adv. Geom., 4, 2004, 279–286.
- A. Grigoriev and G.J. Woeginger, *Project scheduling with irregular costs: complexity, approximability, and algorithms*, Acta Informatica 41(2-3), 2004, 83–97.
- O. Grosek, P. Horak and Trung van Tran, *On non-polynomial Latin squares*, Designs, Codes and Cryptography, 32, 2004, ISSN 0925-1022, 217–226.
- W.H. Haemers and E. Spence, *Enumeration of cospectral graphs*, European Journal of Combinatorics 25, 2004, 199–211.
- W.H. Hamacher, M. Labbé, S. Nickel and T. Sonneborn, *Adapting polyhedral properties from facility to hub location problems*, Discrete Applied Mathematics, 145, 2004, 104–116.
- Jürgen Häring and A.J. Han Vinck, *Coding and signal space diversity for a class of fading and impulsive noise channels*, IEEE Transactions on Information Theory, May 2004, ISSN 0018-9448, 887–895.

- M.I. Hartley and D. Leemans, *Quotients of a universal locally projective polytope of type 5,3,5*, Math. Z. 247, 2004, 663–674.
- T. Helleseth, M. Maas, J.E. Mathiassen and A.J.M. Segers, *Linear complexity over  $F_p$  of Sidel'nikov sequences*, IEEE Transactions on Information Theory, 50(10), 2468–2472.
- W. van Hoeve and M. Milano, *Postponing branching decisions*, in: R.L. de Mántras, L. Saitta (eds.), Proceedings of the 16th European Conference on Artificial Intelligence (ECAI 2004), 2004, 1105–1106.
- W. van Hoeve, G. Pesant and L.-M. Rousseau, *On global warming (softening global constraints)*, in: S. Bistarelli, F. Rossi (eds.), Proceedings of the 6th International Workshop on Preferences and Soft Constraints (held in conjunction with CP 2004), 2004, 1–15, 2004.
- J. Hoogeveen, J. Lenstra and W. Yu, *Minimizing makespan in a two-machine flow shop with delays and unit-time operations is np-hard*, Journal of Scheduling, 7(5), 2004, 333–348.
- J.L. Hurink, G.J.M. Smit and L.T. Smit, *Energy-efficient wireless communication for mobile multimedia terminals*, Radiomatics, 1(1), 2004, 49–58.
- C.A.J. Hurkens and G.J. Woeginger, *On the nearest neighbor rule for the Traveling Salesman Problem*, Operations Research Letters 32(1), 2004, 1–4.
- D. Huygens, A.R. Mahjoub and P. Pesneau, *Two edge-disjoint hop-constrained paths and polyhedra*, SIAM Journal of Discrete Mathematics, 18, 2004, 287–312.
- P. Jacobs and D. Leemans, *An algorithmic analysis of the intersection property*, LMS J. Comput. Math. 7, 2004, 284–299.
- R. Joosten, *Referentiemodel maakt beveiliging inzichtelijk - aanzet tot veilig netwerken met garanties*, TelecomMagazine 9, 2004, 24–27.
- W. Kern and D. Paulusma, *The computational complexity of the elimination problem in generalized sports competitions*, Discrete Optimization, 1, 2004, 205–214.
- B. Klinz and G.J. Woeginger, *Minimum cost dynamic flows: The series-parallel case*, Networks 43(3), 2004, 153–162.
- D. Král, V. Majerech, J. Sgall, T. Tichý and G.J. Woeginger, *It is tough to be a plumber*, Theoretical Computer Science 313(3), 2004, 473–484.
- M. Labbé, G. Laporte, I. Rodriguez Martin and J.J. Salazar, *The ring star problem: Polyhedral analysis and exact algorithm*, Networks, 43, 2004, 177–189.
- M. Labbé, I. Rodriguez Martin and J.J. Salazar, *A branch-and-cut algorithm for the plant-cycle location problem*, Journal of the Operational Research Society, 55, 2004, 513–520.
- M. Labbé and H. Yaman, *Projecting the flow invariants for hub location problems*, Networks, 44, 2004, 84–93.
- Tanja Lange, *Koblitz curve cryptosystems*, Finite Fields and their Applications, online publication 2004.

- Tanja Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, J. AAECC, online publication, 13.11.
- Tanja Lange and Igor Shparlinski, *Collisions in fast generation of ideal classes and points on hyperelliptic and elliptic curves*, J. AAECC, online publication, 13.11.
- M. Laurent, *Semidefinite relaxations for Max-Cut*, volume MP04 of MPS-SIAM Series on Optimization, chapter 16, SIAM Philadelphia, 2004, 257–290.
- D. Leemans, *Constructions of rank five geometries for the Mathieu group  $M_{22}$* , Journal of Geometry, 79, 1-2, 2004, 146–155.
- D. Leemans, *The residually weakly primitive geometries of  $J_3$* , Experiment. Math. 13, 4, 2004.
- J.-D. Legat, G. Piret, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *ICEBERG: an involutinal cipher efficient for block encryption in reconfigurable hardware*, FSE 2004, Lecture Notes in Computer Science, Vol. 3017, Springer-Verlag, February 2004, 279–298.
- J.-D. Legat, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *Compact and efficient encryption/decryption module for FPGA implementation of AES*, Nova Science Publishers, 2004.
- A.K. Lenstra, *Preface (Special issue on Weil pairings)*, Journal of Cryptology, 17(4), 233.
- A.K. Lenstra and T. Voss, *Information security risk assessment, aggregation, and mitigation*, ACISP 2004, Springer-Verlag LNCS 3108, 2004, 391–401.
- J.K. Lenstra, W.E. de Paepe, J. Sgall, R.A. Sitters and L. Stougie, *Computer-aided complexity classification of dial-a-ride problems*, INFORMS Journal on Computing 16(2), 2004, 120–132.
- F. Levy-dit-Vhel and L. Perret, *Attacks on public key cryptosystems based on free partially commutative monoids and groups*, Progress in Cryptology - INDOCRYPT 2004, Lecture Notes in Computer Science, vol. 3348, Springer-Verlag, 2004, 275–289.
- B. Libert and J.-J. Quisquater, *Identity based undeniable signatures*, In: T. Okamoto (ed.), Cryptographer’s Track – RSA 2004, Lecture Notes in Computer Science, vol. 2964, Springer-Verlag, 2004, 112–125.
- B. Libert and J.-J. Quisquater, *Improved signcryption from  $q$ -Diffie-Hellman Problems*, In: C. Blundo (ed.), 4th Conference on Security in Communication Networks’04 (SCN’04), Lecture Notes in Computer Science, vol. 3352, Springer, 2004, 220–234.
- B. Libert and J.-J. Quisquater, *Efficient signcryption with key privacy from Gap Diffie-Hellman Groups*, In: F. Bao (ed.), Public Key Cryptography 2004, Lecture Notes in Computer Science, vol. 2947, Springer-Verlag, 2004, 187–200.
- B. Libert and J.-J. Quisquater, *What is possible with identity based cryptography for PKIs and what still must be improved*, In: S. Katsikas, S. Gritzalis and J. Lopez (eds.), First European PKI Workshop (EuroPKI’04), Lecture Notes in Computer Science, Springer, 2004, 57–70.

- M. Lipmann, X. Lu, W.E. de Paepe, R.A. Sitters, L. Stougie, *On-line dial-a-ride problems under a restricted information model*, *Algorithmica* 40(4), 2004, 319–329.
- D. Luyckx and J.A. Thas, *Semipartial geometries, arising from locally hermitian 1-systems of  $W_5(q)$* , *Bulletin of the Belgian Mathematical Society*, 11(1), 2004, 69–76.
- D. Luyckx and J. A. Thas, *Locally Hermitian 1-systems of  $Q^+(7, q)$* , *Discrete Mathematics* 282, 2004, 223–231.
- H. Van Maldeghem and T. De Medts, *Moufang generalized polygons*, in: *Topics in Diagram Geometry*, *Quaderni di Matematica*, 12, 2004, 59–126.
- H. Van Maldeghem and A. Offer, *Spreads and ovoids translation with respect to disjoint flags*, *Designs, Codes and Cryptography*, 32, 2004, 351–367.
- H. Van Maldeghem and A. Steinbach, *Regular embeddings of generalized hexagons*, *Canadian Journal of Mathematics*, 56, 2004, 1068–1093.
- H. Van Maldeghem and J. A. Thas, *Full embeddings of the finite dual split Cayley hexagons*, *Combinatorica*, 24, 2004, 681–698.
- H. Van Maldeghem and J.A. Thas, *Classification of finite Veronesean caps*, *European Journal of Combinatorics* 25, 2004, 275–285.
- H. Van Maldeghem and J.A. Thas, *Characterizations of the finite quadric Veroneseans  $V_n^{2^n}$* , *Quart. J. Oxford*, 55, 2004, 99–113.
- H. Van Maldeghem and J.A. Thas, *Some characterizations of finite Hermitian Veroneseans*, *Designs, Codes and Cryptography*, preprint.
- H. Van Maldeghem and A. De Wispelaere, *A distance-2-spread of the generalized hexagon  $H(3)$* , *Annals of Combinatorics* 8, 2004, 133–154.
- S. Martirosyan and Trung van Tran, *On a class of traceability codes*, *Designs, Codes and Cryptography*, 31, 2004, ISSN 0925-1022, 125–132.
- S. Martirosyan and Trung van Tran, *On  $t$ -covering arrays*, *Designs, Codes and Cryptography*, 32, 2004, ISSN 0925-1022, 323-339.
- T. De Medts, *Automorphisms of  $F_4$  quadrangles*, *Math. Ann.* 328, 2004, 399–413.
- S.B. Ors, B. Preneel and F.-X. Standaert, *Power analysis of an FPGA implementation of Rijndael: Is pipelining a DPA countermeasure?*, *CHES2004*, *Lecture Notes in Computer Science*, Springer-Verlag, 2004, 30–44.
- S.B. Ors, B. Preneel, J.-J. Quisquater and F.-X. Standaert, *Power analysis attacks against FPGA implementations of the DES*, *FPL 2004*, *Lecture Notes in Computer Science*, Springer-Verlag, 2004, 84–94.
- M. Neve, E. Peeters, J.-J. Quisquater and F.-X. Standaert, *L'émission rayonnée des cartes à puces: une vue d'ensemble*, In: *Revue de l'Electricité et de l'Electronique*, June/July 2004.
- G.R. Pellikaan and X.W. Wu, *List decoding of  $q$ -ary Reed-Muller codes*, *IEEE Transactions on Information Theory*, 50(4), April 2004, 679–682.

- O. Pereira and J.-J. Quisquater, *Generic insecurity of cliques-type authenticated group key agreement protocols*, Proceedings of the 17th IEEE Computer Security Foundations Workshop – CSFW-17, IEEE Computer Society Press, June 2004, 16–29.
- Y. Pochet and M. Van Vyve, *A general heuristic for production planning problems*, INFORMS Journal on Computing, 16, 2004, 316–327.
- J.-J. Quisquater and F.-X. Standaert, *Time-memory tradeoffs*, Encyclopedia of Cryptography and Security, Springer-Verlag, 2004.
- R. Rosenthal and G.J. Woeginger, *Eine Balkenwaage und eine Pell'sche Gleichung*, Wissenschaftliche Nachrichten 126, 23, 2004.
- Y. Shtarkov, T.J. Tjalkens and F.M.J. Willems, *Optimal universal coding with respect to the maximal individual relative redundancy criterion*, Problems in Information Transmission, 40, 1, 2004, 90-101.
- J.L. Simons and B.M.M. de Weger, *Mersenne en het Syracuseprobleem*, Nieuw Archief voor Wiskunde, 5(3), 2004, 218–220.
- G.J. Still, *Solving generalized semi-infinite programs by reduction to simpler problems*, Optimization, 53(1), 2004, 19–34.
- L. Storme and A. De Vos, *r-Universal reversible logic gates*, J. Phys. A: Math. and Gen., 37, 2004, 5815–5824.
- R.J. Stroeker and B.M.M. de Weger, *On integral zeroes of binary Krawtchouk polynomials*, In: Development of the mathematical ideas of Mykhailo Kravchuk (Krawtchouk), Shevchenko Scientific Society (USA), New York, and National Technical University of Ukraine "KPI", Kyiv, 2004, 623–633. (reprint from Nieuw Archief voor Wiskunde (4), 17(2):175-186, 1999.
- INengah Suparta and A.J. van Zanten, *Totally balanced and exponentially balanced Gray codes*, Discrete Analysis and Operation Research, 11, 2004, 62–79.
- J.A. Thas and S. De Winter, *SPG-reguli satisfying the polar property and a new semipartial geometry*, Designs, Codes and Cryptography, 32, 1-3, 2004, 153–166.
- K. Thas, *On a conjecture of W.M. Kantor, and strongly irreducible groups acting on generalized quadrangles*, Forum Math., 16, 2004, 671–679.
- K. Thas, *Symmetry in Finite Generalized Quadrangles*, Monograph, Frontiers in Mathematics, 1, Birkhäuser-Verlag, Basel, Boston, Berlin, 2004, ISBN 3-7643-6158-1.
- Pim Tuyls and Berry Schoenmakers, *Practical two-party computation based on the conditional gate*, Advances in Cryptology-ASIACRYPT'04, Lecture Notes in Computer Science, 3329, Berlin, Springer-Verlag 2004, 119–136.
- M. Van Vyve and F. Ortega, *Lot-sizing with fixed charges on stocks: the convex hull*, Discrete Optimization, 1, 2004, 189–203.
- S. De Winter, *Elation and translation semipartial geometries* J. Combin. Theory Ser. A **108** (2004), no. 2, 313–330.
- G.J. Woeginger, *Approximations through relaxations*, Nieuwsbrief van de Nederlandse Vereniging voor Theoretische Informatica, 8, 2004, 12–18.

- G.J. Woeginger, *Open problems in the theory of scheduling*, In: Current Trends in Theoretical Computer Science, G. Paun, G. Rozenberg and A. Salomaa (eds.), 2004, 19–38.
- G.J. Woeginger, *Inapproximability results for no-wait job shop scheduling*, Operations Research Letters 32(4), 2004, 320–325.
- G.J. Woeginger, *Seventeen lines and one-hundred-and-one points*, Theoretical Computer Science 321(2-3), 2004, 415–421.

### 4.3 Research articles awaiting publication

- P. Abramenko and H. Van Maldeghem, *Combinatorial characterizations of convexity and apartments in buildings*, to appear in Australasian Journal of Combinatorics.
- A. Aguglia, G.L. Ebert and D. Luyckx, *On partial ovoids of Hermitian surfaces*, Bulletin of the Belgian Mathematical Society, to appear.
- C. Archer, *The firm RWPri geometries of supersoluble groups*, Atti Seminario Matematico e Fisicom Univ. Modena, to appear.
- C. Archer, Ph. Cara and J. Krempa, *Using the Frattini subgroup and independent sets to study RWPRI geometries*, Beiträge zur Algebra und Geometrie, to appear.
- S. Ball, P. Govaerts and L. Storme, *On ovoids of parabolic quadrics*, Designs, Codes and Cryptography, to appear.
- J. De Beule, P. Govaerts and L. Storme, *PG – Projective Geometries, a share package for GAP*, submitted.
- J. De Beule and K. Metsch, *Minimal blocking sets of size  $q^2 + 2$  of  $Q(4, q)$ ,  $q$  an odd prime, do not exist*, Finite Fields Appl., to appear.
- J. De Beule and K. Metsch, *The smallest minimal blocking sets of  $H(2n, q^2)$* , Discrete Mathematics, to appear.
- J. De Beule and K. Metsch, *The Hermitian variety  $H(5, 4)$  has no ovoid*, Bulletin of the Belgian Mathematical Society Simon Stevin, to appear.
- J. De Beule and L. Storme, *The two smallest minimal blocking sets of  $Q(2n, 3)$ ,  $n \geq 3$* , Bulletin of the Belgian Mathematical Society, Proceedings of the International Conference on Incidence Geometry, La Roche-en-Ardenne, Belgium, May 23-29, 2004, to appear.
- J. De Beule and L. Storme, *On the smallest minimal blocking sets of  $Q(2n, q)$ , for  $q$  an odd prime*, Discrete Mathematics, Proceedings of Finite Geometries, First Irsee Conference, Kloster Irsee, Germany (February 16-21, 2003), to appear.
- P.S. Bonsma, Th. Epping and W. Hochstättler, *Complexity results on restricted instances of a paint shop problem for words*, to appear in DAM.
- S. Brandt, H.J. Broersma, R. Diestel and M. Kriesell, *Global connectivity and expansion: long cycles and factors in  $f$ -connected graphs*, to appear in Combinatorica.
- G. Brinkmann and B.D. McKay, *Counting unlabeled topologies and transitive relations*, Journal of Integer Sequences, to appear.

- H.J. Broersma, F. Fomin, J. Kratochvíl and G. Woeginger, *Planar graph coloring avoiding monochromatic subgraphs: trees and paths make it difficult*, to appear in *Algorithmica*.
- H.J. Broersma, C.A. Rodger and A.N.M. Salman, *More on spanning 2-connected subgraphs of alphabet graphs, special classes of grid graphs*, accepted for publication in *Bulletin of the Institute of Combinatorics and Its Applications*.
- H.J. Broersma, Z. Ryjáček and L. Xiong, *On stability of the Hamiltonian index under contractions and closures*, to appear in *Journal of Graph Theory*.
- H.J. Broersma and A.N.M. Salman, *Path-fan Ramsey numbers*, accepted for publication in *Discrete Applied Mathematics*.
- H.J. Broersma and A.N.M. Salman, *On Ramsey numbers for paths versus wheels*, accepted for publication in *Discrete Applied Mathematics*.
- H.J. Broersma and L. Xiong, *Subpancyclicity of line graphs and degree sums along paths*, to appear in *Discrete Applied Mathematics*.
- H.J. Broersma, L. Xiong and K. Yoshimoto, *Toughness and Hamiltonicity in  $k$ -trees*, to appear in *Discrete Mathematics*.
- A.E. Brouwer, P.J. Cameron, W.H. Haemers and D.A. Preece, *Self-dual, not self-polar*, to appear in *Discrete Mathematics*.
- A.E. Brouwer, A.M. Cohen and M.V.M. Nguyen, *Orthogonal arrays of strength 3 and small run sizes*, *J. Stat. Planning Inf.*, accepted.
- A.E. Brouwer and W.H. Haemers, *Eigenvalues and perfect matchings*, to appear in *Linear Algebra and its Applications*.
- B. De Bruyn, *Association schemes based on some regular near hexagons*, to appear in *Discrete Mathematics, Proceedings of the Fourth Shanghai Conference on Combinatorics*.
- B. De Bruyn, *Slim near polygons*, to appear in *Designs, Codes and Cryptography*.
- B. De Bruyn, *Dense near polygons with two types of quads and three types of hexes*, to appear in *Journal of Combinatorial Mathematics and Combinatorial Computing*.
- B. De Bruyn and P. Vandecasteele, *Valuations and hyperplanes of dual polar spaces*, to appear in *Journal of Combinatorial Theory, Series A*.
- M. Čajková and V. Fack, *Clique algorithms for classifying substructures in generalized quadrangles*, *Electronic Notes in Discrete Mathematics*, to appear.
- Sébastien Canard, Berry Schoenmakers, Martijn Stam, and Jacques Traoré, *List signature schemes*, *Discrete Applied Mathematics*, to appear.
- P.-E. Caprace and B. Mühlherr, *Isomorphisms of Kac-Moody groups*, accepted for *Inv. math.*
- P.-E. Caprace and B. Mühlherr, *Reflection triangles in Coxeter groups and biautomaticity*, accepted for *J. Group Theory*.

- P.-E. Caprace and B. Mühlherr, *Reflection rigidity of 2-spherical Coxeter groups*, accepted for Proceedings of the London Mathematical Society.
- Ph. Cara and D. Leemans, *On inductively minimal geometries that satisfy the intersection property*, Journal of Combinatorial Theory Series A, to appear, 4 pages.
- F. De Clerck, N. Durante, N. De Feyter, *Two-intersection sets with respect to lines on the Klein quadric*, to appear in Bulletin of the Belgian Mathematical Society Simon Stevin, Proceedings of Incidence Geometry, International Conference at La Roche, Belgium.
- F. De Clerck, N. De Feyter and, J.A. Thas, *Affine embeddings of  $(0, \alpha)$ -geometries*, to appear in European Journal of Combinatorics.
- F. De Clerck, E. Kuijken, C. Tonesi and S. De Winter, *Distance-regular  $(0, \alpha)$ -reguli*, to appear in Designs, Codes and Cryptography.
- A.M. Cohen and E.J. Postma, *Covers of point-hyperplane graphs*, 2004, to appear.
- K. Coolsaet, *A distance regular graph with intersection array  $(21, 16, 8; 1, 4, 14)$  does not exist*, European Journal of Combinatorics, to appear.
- K. Coolsaet and J. Degraer, *A computer assisted proof of the uniqueness of the Perkel graph*, Designs, Codes and Cryptography, to appear.
- J.G. Cederquist, R. Corin, M.A.C. Dekker, S. Etalle en J.I den Hartog, *An audit logic for accountability*, IEEE 6th International Workshop on Policies for Distributed Systems and Networks, accepted.
- E.R. van Dam, *The combinatorics of Dom de Caen*, to appear in Designs, Codes and Cryptography.
- E.R. van Dam and J.H. Koolen, *A new family of distance-regular graphs with unbounded diameter*, to appear in Inventiones Mathematicae.
- E.R. van Dam and E. Spence, *Combinatorial designs with two singular values II*, to appear in Partial geometric designs, Linear Algebra and its Applications.
- T.S.H. Driessen and H. Meinhardt, *Convexity of production, common pool and oligopoly games: a survey*, to appear.
- T.S.H. Driessen and H. Meinhardt, *Stability of cartels and the incentive for merger in oligopoly situations without transferable technologies*, to appear in Mathematical Social Sciences.
- D. Van Dyck and V. Fack, *On the reduction of Yutsis graphs*, Discrete Mathematics, to appear.
- D. Van Dyck and V. Fack, *To be or not to be Yutsis*, Electronic Notes in Discrete Mathematics, to appear.
- J. Eisfeld, L. Storme and P. Sziklai, *On the spectrum for the sizes of maximal partial line spreads in  $PG(2n, q)$ ,  $n \geq 3$* , Designs, Codes and Cryptography, to appear.
- N.C. Fiala and W.H. Haemers, *5-Chromatic strongly regular graphs*, to appear in Discrete Mathematics.

- S. Ferret and L. Storme, *A classification result on weighted  $\{\delta v_{\mu+1}, \delta v_{\mu}; N, p^3\}$ -minihypers*, Discrete Applied Mathematics, to appear.
- N. De Feyter, *The embedding in  $AG(3, q)$  of  $(0, 2)$ -geometries with no planar nets*, Journal of Combinatorial Theory, to appear.
- N. De Feyter, *The embedding in  $AG(3, q)$  of  $(0, 2)$ -geometries containing a planar net*, to appear in Discrete Mathematics.
- N. De Feyter, *The embedding of  $(0, 2)$ -geometries and semipartial geometries in  $AG(n, q)$* , to appear in Adv. Geometry.
- J. Fiala and D. Paulusma, *A complete complexity classification of the role assignment problem*, Theoretical Computer Science, to appear.
- S. Fiorini,  *$0, 1/2$ -cuts and the linear ordering problem: surfaces that define facets*, accepted pending revision for publication in SIAM Journal on Discrete Mathematics.
- P. Govaerts, *Small maximal partial  $t$ -spreads*, Bulletin of the Belgian Mathematical Society Simon Stevin, to appear.
- P. Govaerts and T. Penttila, *Cameron-Liebler line classes in  $PG(3, 4)$* , Bulletin of the Belgian Mathematical Society Simon Stevin, to appear.
- T. Grundhöfer and H. Van Maldeghem, *Sharp homogeneity in affine planes, and in some affine generalized polygons*, to appear Abh. Math. Sem. Univ. Hamburg.
- I. Gutman, P. Hansen and H. Mélot, *Variable neighborhood search for extremal graphs 12. A note on the Variance of bounded degrees in graphs*, MATCH Comm. Math. Comp. Chem., accepted.
- I. Gutman, P. Hansen and H. Mélot, *Variable neighborhood search for extremal graphs 10. Comparison of irregularity indices for chemical trees*, J. Chem. Inf. Comput. Sci, to appear.
- W.H. Haemers, *Conditions for singular incidence matrices*, to appear in Journal of Algebraic Combinatorics.
- W.H. Haemers, *Matrices and Graphs*, to appear in "Handbook of Linear Algebra", CRC Press.
- N. Hamilton and J.A. Thas, *Maximal arcs in  $PG(2, q)$  and partial flocks of the quadratic cone*, Advances in Geometry, to appear.
- P. Hansen, M. Aouchiche, G. Caporossi, H. Mélot and D. Stevanović, *What forms do interesting conjectures have in graph theory*, In: S. Fajtlowicz et al. (eds.), Graphs and Discovery, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Providence, American Mathematical Society, to appear.
- P. Hansen and H. Mélot, *Variable neighborhood search for extremal graphs 9. Bounding the irregularity of a graph*, In: S. Fajtlowicz et al. (eds.), Graphs and Discovery, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Providence, American Mathematical Society, to appear.
- F. Haot and H. Van Maldeghem, *A half 3-Moufang quadrangle is Moufang*, to appear in Bulletin of the Belgian Mathematical Society Simon Stevin.

- F. Haot, H. Van Maldeghem, T. De Medts and K. Tent, *Split BN-pairs of rank at least 2 and the uniqueness of splittings*, accepted for publication in J. Group Theory, 10 pages.
- M.I. Hartley and D. Leemans, *On the rank four thin regular geometries of the Janko group  $J_1$* , Innovations in Incidence Geometry, to appear, 9 pages.
- J.L. Hurink and S. Knust, *Tabu search algorithms for job-shop problems with a single transport robot*, to appear in European Journal of Operational Research.
- D. Jibeteau and E. de Klerk, *Global optimization of rational functions: a semidefinite programming approach*, accepted for publication in Mathematical Programming, Series A.
- D. Jibeteau and M. Laurent, *Semidefinite approximations for global unconstrained polynomial optimization*, Accepted for publication in the SIAM Journal on Optimization.
- J. De Kaey, *A characterization of the Split Cayley Generalized Hexagon  $H(q)$  using one subhexagon of order  $(1, q)$* , to appear in Elsevier Science.
- J. De Kaey and H. Van Maldeghem, *A characterization of the split Cayley generalized hexagon  $H(q)$  using one subhexagon of order  $(1, q)$* , to appear in Discrete Mathematics.
- E. Kuijken and C. Tonesi, *Distance-regular graphs and  $(\alpha, \beta)$ -geometries*, to appear in Journal of Geometry.
- M. Labbé, G. Laporte, I. Rodriguez Martin and J.J. Salazar, *Locating median cycles in networks*, European Journal of Operational Research, to appear.
- M. Labbé, H. Yaman and E. Gourdin, *A branch and cut algorithm for hub location problems with single assignment*, Mathematical Programming, to appear.
- Tanja Lange and Igor Shparlinski, *Certain exponential sums and random walks on elliptic curves*, to appear in Canadian Journal of Mathematic.
- Tanja Lange and Marc Stevens, *Efficient doubling on genus two curves over binary fields*, accepted for Workshop on Selected Areas in Cryptography SAC2004.
- D. Leemans, *The residually weakly primitive geometries of  $HS$* , Australasian Journal of Combinatorics, to appear, 6 pages.
- D. Leemans, *The residually weakly primitive geometries of  $M_{23}$* , Atti Sem. Mat. Fis. Univ. Modena, to appear, 4 pages.
- D. Leemans, *A generalization of a construction due to Van Nypelseer*, Beitrage Algebra Geom., to appear, 15 pages.
- D. Leemans, *A family of geometries related to the Suzuki tower*, Comm. Algebra, to appear, 15 pages.
- D. Leemans, *Two rank six geometries for the Higman-Sims sporadic group*, Proceedings of the First Irsee Conference on Finite Geometries (Irsee), Discrete Mathematics, to appear, 10 pages.

- A.K. Lenstra, *Key lengths, contribution to The Handbook of Information Security*, Wiley, 2004, to appear.
- D. Luyckx and J.A. Thas, *Trialities and 1-systems of  $Q^+(7, q)$* , Designs, Codes and Cryptography, to appear.
- D. Luyckx and J.A. Thas, *The uniqueness of the 1-system of  $Q^-(7, q)$ ,  $q$  even*, Discrete Mathematics, to appear.
- H. Van Maldeghem and A. Offer, *Distance- $j$  ovoids and related structures in generalized polygons*, to appear in Discrete Mathematics.
- H. Van Maldeghem, A. Offer and K. Thas, *Generalized quadrangles with an ovoid that is translation with respect to opposite flags*, to appear in Arch. Math.
- H. Van Maldeghem and J.A. Thas, *Some characterizations of finite Hermitian Veroneseans*, to appear in Designs, Codes and Cryptography.
- H. Van Maldeghem and J.A. Thas, *On Ferri's characterization of the finite quadric Veronesean  $V_2^4$* , to appear in Journal of Combinatorial Theory, Series A.
- H. Van Maldeghem and J.A. Thas, *Generalized polygons in finite projective spaces*, to appear in Proceedings 2004 Com<sup>2</sup>MaC Workshop on Distance-Regular Graphs and Finite Geometry, Busan, Korea.
- H. Van Maldeghem and J.A. Thas, *Finite Moufang generalized quadrangles*, to appear in Proc. Int. Conf. on "Geometric and Group Theory Methods in Physics and Mathematics", Batumi (Georgia), September 15-27, 2003, Math. Sci. Plenum Publ. Co (Russian version in Itogi Nauki I Tehniki).
- H. Van Maldeghem and A. De Wispelaere, *Some new two-character sets in  $PG(5, q^2)$  and a distance-2-ovoid in the generalized hexagon  $H(4)$* , accepted in Discrete Mathematics.
- H. Van Maldeghem and A. De Wispelaere, *A Holz-design in the generalized hexagon  $H(q)$* , accepted in The Bulletin of The Belgian Mathematical Society - Simon Stevin.
- H. Van Maldeghem and A. De Wispelaere, *Some new two-character sets in  $PG(5, q^2)$  and a distance-2-ovoid in the generalized hexagon  $H(4)$* , to appear in Discrete Mathematics.
- T. De Medts, *Algebraic inclusions of Moufang polygons*, accepted for publication in Forum Math., 34 pages.
- T. De Medts, *Inclusions of spherical buildings of equal rank*, accepted for publication in Bulletin of the Belgian Mathematical Society Simon Stevin, 15 pages.
- T. De Medts, *An algebraic structure for Moufang quadrangles*, Memories of the American Mathematical Society, to appear.
- B. Mühlherr and A. Nguyen, *A combinatorial approach to Coxeter groups*, Bulletin of the Belgian Mathematical Society, to appear.
- INengah Suparta and A.J. van Zanten, *On the construction of linear  $q$ -ary lexicode*s, Codes, Designs and Cryptography, to appear.

- S.E Payne and J.A. Thas, *The stabilizer of the Adelaide oval*, Discrete Mathematics, to appear.
- Y. Van Rentergem, L. Storme and A. De Vos, *Implementing an arbitrary reversible logic gate*, J. Phys. A: Math. and Gen., to appear.
- L.A.M. Schoenmakers and P. Tuyls, *Private profile matching*, Proceedings Symposium of Intelligent Algorithms (SOIA'04), to appear.  
L.A.M. Schoenmakers and P. Tuyls, *Practical two-party computation based on the conditional gate*, to appear in Advances in Cryptography, Asiacrypt 2004, LNCS 3329, Springer-Verlag, Berlin, 119-136, 2004.
- John Simons and Benne de Weger, *Theoretical and computational bounds for  $m$ -cycles of the  $3n + 1$ -problem*, Acta Arithmetica, to appear.
- L. Storme, *Linear codes meeting the Griesmer bound, minihypers, and geometric applications*, Le Matematiche, to appear.
- J.A. Thas, *Finite geometries: classical problems and recent developments*, Rend. di Mat., to appear.
- J.A. Thas and K. Thas, *Translation generalized quadrangles and translation duals*, Part 1, Discrete Mathematics, to appear.
- J.A. Thas and S. De Winter, *On semi-pseudo-ovals*, to appear in Journal of Algebraic Combinatorics.
- K. Thas, *Elation generalized quadrangles of order  $(q, q^2)$ ,  $q$  even, with a classical subGQ of order  $q$  containing the elation point are classical*, to appear in Adv. Geom.
- K. Thas, *Some basic questions and conjectures on elation generalized quadrangles, and their solutions*, to appear in Bulletin of the Belgian Mathematical Society Simon Stevin.
- K. Thas, *Generalized quadrangles admitting  $PSL(2, q) \times PSL(2, q)$* , to appear in Journal of Combinatorial Designs.
- K. Thas and S. E. Payne, *Foundations of elation generalized quadrangles*, to appear in European Journal of Mathematics.
- M. Van Vyve, *The continuous mixing polyhedron*, Mathematics of Operations Research, to appear.
- M. Van Vyve, *Linear programming extended formulations for the single-item lot-sizing problem with backloging and constant capacity*, to appear.
- M. Van Vyve and L.A. Wolsey, *Approximate extended formulations*, Mathematical Programming B, to appear.
- S. De Winter, *Linear representations of semipartial geometries*, to appear in Bulletin of the Belgian Mathematical Society Simon Stevin.

#### 4.4 Research articles submitted for publication

- Claude Archer, *Reduction of the extension problem to a soluble group*, submitted.
- G. Van Assche, J. Cardinal and S. Fiorini, *On minimum entropy graph colorings*, submitted.
- J. De Beule and L. Storme, *Blocking all generators of  $Q^+(2n+1, 3)$ ,  $n \geq 4$* , Designs, Codes and Cryptography, submitted.
- D. Bokal, G. Brinkmann and S. Grünewald, *Chromatic index critical graphs of orders 13 and 14*, submitted.
- O. Borodin, H.J. Broersma, A. Glebov and J. van den Heuvel, *A new upper bound on the cyclic chromatic number*, Journal of Graph Theory, submitted.
- Nicolas Bougard, *Orbits on vertices and edges in finite regular graphs*, Journal of Graph Theory, submitted.
- Nicolas Bougard, *The Lotto numbers  $L(n, 3, p, 2)$* , Journal of Combinatorial Designs, submitted.
- G. Brinkmann and B.D. McKay, *Construction of planar triangulations with minimum degree 5*, submitted.
- G. Brinkmann, S. Greenberg, C. Greenhill, B.D. McKay, R. Thomas and P. Wollan, *Generation of simple quadrangulations of the sphere*, submitted.
- H.J. Broersma, Fedor V. Fomin, Rastislav Kralovic and Gerhard J. Woeginger, *Eliminating graphs by means of parallel knock-out schemes*, Discrete Applied Mathematics, submitted.
- H.J. Broersma, J. Fujisawa, L. Marchal, D. Paulusma, A.N.M. Salman and K. Yoshimoto, *Lambda-backbone colorings along pairwise disjoint stars and matchings*, Graphs and Combinatorics, submitted.
- H.J. Broersma and A.N.M. Salman, *Path-kipas Ramsey numbers*, Discrete Applied Mathematics, submitted.
- L. Brotcorne, M. Labbé, P. Marcotte and G. Savard, *Joint design and pricing on a network*, submitted.
- A.E. Brouwer, G. Horváth, I. Molnár-Sáska and C. Szabó, *Chomp*, preprint, submitted.
- M.R. Brown, H. Van Maldeghem, and C. Tonesi, *A group theoretic approach to  $(0, 2)$ -geometries*, submitted.
- J. Christophe, S. Dewez, J.-P. Doignon, S. Elloumi, G. Fasbender, P. Grégoire, D. Huygens, M. Labbé, H. Mélot and H. Yaman, *Linear inequalities among graph invariants: using GraPHedron to uncover optimal relationships*, submitted.
- M. Cimráková and V. Fack, *Searching for maximal partial ovoids and spreads in generalized quadrangles*, Bulletin of the Belgian Mathematical Society Simon Stevin, submitted.

- M. Cimráková and V. Fack, *Clique algorithms for finding substructures in generalized quadrangles*, Discrete Applied Mathematics, submitted.
- M. Cimráková, V. Fack, L. Storme and S. De Winter, *On the smallest maximal partial ovoids and spreads of the generalized quadrangles  $W(q)$  and  $Q(4, q)$* , Journal of Combinatorial Theory, Series A, submitted.
- K. Coolsaet, *The uniqueness of the strongly regular graph  $srg(105, 32, 4, 12)$* , Bulletin of the Belgian Mathematical Society Simon Stevin, submitted.
- J. Correau, S. Fiorini and N. Stier-Moses, *A note on the precedence-constrained class sequencing problem*, submitted.
- E.R. van Dam, W.H. Haemers, J.H. Koolen, and E. Spence, *Characterizing distance-regularity of graphs by the spectrum*, submitted.
- E.R. van Dam, D. den Hertog and B.G.M. Husslage, *One-dimensional nested maximin designs*, submitted.
- E.R. van Dam, D. den Hertog, B.G.M. Husslage and J.B.M. Melissen, *Maximin Latin hypercube designs in two dimensions*, submitted.
- J. Degraer and K. Coolsaet, *Classification of three-class association schemes using backtracking with dynamic variable ordering*, Discrete Mathematics, submitted.
- J. Degraer and K. Coolsaet, *Classification of some strongly regular subgraphs of the McLaughlin graph*, Discrete Mathematics, submitted.
- A. Devillers, *A classification of finite partial linear spaces with a primitive rank 3 automorphism group of almost simple type or of grid type*, submitted.
- J.-P. Doignon, S. Elloumi, G. Fasbender, P. Grégoire, D. Huygens, M. Labbé, H. Mélot, J. Christophe, S. Dewez and H. Yaman, *Linear inequalities among graph invariants: using GraPHedron to uncover optimal relationships*, submitted.
- T.S.H. Driessen, *Associated consistency and values for TU games*, International Journal Game Theory, submitted.
- Y. Edel, L. Storme and P. Sziklai, *New upper bounds for the sizes of caps in  $PG(N, 5)$  and  $PG(N, 7)$* , Journal of Combinatorial Mathematics and Combinatorial Computing, submitted.
- M. Ernst, E. Jochemsz, A. May and B. de Weger, *Partial key exposure attacks on RSA up to full size exponents*, submitted to EuroCrypt 2005.
- N. De Feyter, *Classification of  $(0, 2)$ -geometries embedded in  $AG(3, q)$* , Designs, Codes and Cryptography, submitted.
- S. Fiorini, *How to recycle your facets*, submitted.
- H. Fleuren, M.G.C. van Krieken and R. Peeters, *Problem reduction in set partitioning problems*, submitted.
- A. Gottcheiner and D. Leemans, *On the structure of solvable non-supersolvable groups*, submitted, 9 pages.
- R. Gramlich and H. Van Maldeghem, *Intransitive flipflop geometries*, submitted.

- F. Haot, R. Knop, H. Van Maldeghem and T. De Medts, *On the uniqueness of the unipotent subgroups of some Moufang sets*, submitted.
- J. Huizinga, H. Van Maldeghem and A. De Wispelaere, *Ovoids and spreads of the generalized hexagon  $H(3)$* , submitted to Discrete Mathematics.
- D. Huygens, A.R. Mahjoub and P. Pesneau, *On the  $k$  edge disjoint 2-hop-constrained paths polytope*, Operation Research Letters, submitted.
- J.C.M. Keijsper, R.A. Pendavingh and L. Stougie, *A linear programming formulation of Mader's edge-disjoint paths problem (revised version)*, Journal of Combinatorial Theory Series B, submitted.
- M. Labbé and H. Yaman, *Polyhedral analysis for concentrator location problems*, submitted.
- M. Labbé and H. Yaman, *Solving the uncapacitated concentrator location problem with star routing*, submitted.
- Gregor Leander, *Construction bent functions via Niho-power functions*, submitted.
- D. Luyckx, *On maximal partial spreads of  $H(2n + 1, q^2)$* , submitted to Discrete Mathematics.
- H. Van Maldeghem and B. Mühlherr *Moufang sets from groups of mixed type*, submitted.
- H. Van Maldeghem and M. Stroppel, *Automorphisms of unitals*, submitted.
- H. Van Maldeghem and J. A. Thas, *Embeddings of small generalized polygons*, submitted.
- H. Van Maldeghem and K. Thas, *Geometrical characterizations of finite Chevalley groups of type  $B_2$* , 43 pp., submitted to Transactions of the American Mathematical Society.
- H. Van Maldeghem and K. Thas, *Geometric characterizations of finite Chevalley groups of type  $B_2$* , submitted.
- H. Van Maldeghem and A. De Wispelaere, *Codes of generalized hexagons*, submitted to Designs, Codes and Cryptography.
- T. De Medts and R. Weiss, *Moufang sets and Jordan division algebras*, submitted.
- B. Mühlherr *The isomorphism problem for Coxeter groups*, submitted.
- A. Nguyen and B. Mühlherr *A combinatorial approach to Coxeter groups*, submitted.
- L. Storme, *Weighted  $\{\delta(q + 1), \delta; k - 1, q\}$ -minihypers*, Discrete Mathematics, Proceedings of Combinatorics '04, Capomulini, Italy (September 13–18, 2004), submitted.
- J.A. Thas and K. Thas, *Translation generalized quadrangles: old results, new results, open problems*, 14 pp., submitted to Proceedings of the Pingree Park conference “Finite Geometries, Groups and Computation”.

- J.A. Thas and K. Thas, *Translation generalized quadrangles in even characteristic*, Advances in Mathematics, preprint.
- J.A. Thas and K. Thas, *Finite translation generalized quadrangles: old results, new results, open problems*, Proceedings of the Conference “Finite Geometries, Groups and Computation”, Pingree Park Colorado 2004, De Gruyter “Proceedings in Mathematics”, preprint.
- K. Thas, *On the number of points of a hypersurface in finite projective space* (after J.-P. Serre), 9 pp., submitted to Journal of Algebraic Geometry.
- K. Thas, *Determination of elation generalized quadrangles with distinct elation points*, 25 pp., submitted to Quart. J. Math. (Oxford).
- K. Thas, *A stabilizer lemma for translation generalized quadrangles*, 23 pp., submitted to European Journal of Mathematics.
- K. Thas, *A remark concerning certain union-closed families*, 5 pp., submitted to Discrete Mathematics.
- K. Thas, *Generalized quadrangles of order  $(p, t)$  with a 2-transitive regulus,  $p$  a prime*, 10 pp., submitted to Journal of Combinatorial Theory, Series A.
- K. Thas, *Topics in finite and algebraic geometry*, 72 pp., submitted to Atti Sem. Mat. Fis. Univ. Modena.
- K. Thas, *Combinatorial bounds for the number of rational points of a hypersurface*, 12 pp., Appendix to “Topics in finite and algebraic geometry”, submitted.
- K. Thas and S. De Winter, *Generalized quadrangles with an Abelian Singer group*, submitted to Designs, Codes and Cryptography.

#### 4.5 Conference Proceedings

- N. Aboudagga, D. Giry and J.-J. Quisquater, *Wireless security design overview*, In: R. Pellikaan (ed.), Twenty-fifth Symposium on Information Theory in the Benelux, WIC, June 2004, 153–160.
- A. Adelsbach, S. Gajek and J. Schwenk, *Visual spoofing of SSL protected web sites and effective countermeasures*, accepted for the First Information Security Practice and Experience Conference (ISPEC 2005), April 11-14, 2005, Singapore.
- A. Adelsbach, U. Greveler and J. Schwenk, *Fair DRM - Ermoglichen von Privatkopien und Schutz digitaler Waren*, accepted for 9. Deutscher IT-Sicherheitskongress des BSI, May 2005.
- A. Adelsbach, U. Huber and A.-R. Sadeghi, *Secure software delivery and installation in embedded systems*, accepted for the First Information Security Practice and Experience Conference (ISPEC 2005), April 11-14, 2005, Singapore.
- A. Adelsbach, M. Rohe and A.-R. Sadeghi *Overcoming the obstacles of zero-knowledge watermark detection*, ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, 46–55, 2004.

- A. Adelsbach and J. Schwenk, *Key-assignment strategies for CPPM*, ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, 46–55, 2004.
- Gilles Van Assche, Jean Cardinal and Samuel Fiorini, *On minimum entropy graph colorings*, In: Proceedings IEEE International Symposium on Information Theory (ISIT), 2004.
- Gilles Van Assche, Jean Cardinal and Samuel Fiorini, *A graph coloring problem with applications to data compression*, Technical Report 517, Computer Science Department, Université Libre de Bruxelles, Belgium, 2004.
- R. Avanzi, *A note on the signed sliding window integer recoding and a left-to-right analogue*, SAC 2004.
- R. Avanzi, *Aspects of hyperelliptic curves over large prime fields in software implementations*, CHES 2004.
- S. Baggen, V.B. Balakirsky, S. Egner, H. Hollmann and L. Tolhuizen, *On the entropy rate of a hidden Markov model*, Proceedings of the IEEE Symposium on Information Theory, ISIT'2004, June 26 - July 2, 2004, p. 12.
- A. Bayad and L. Perret, *a differential approach to a polynomial equivalence problem*, Proceedings of the IEEE International Symposium on Information Theory (ISIT 2004), 2004.
- V.B. Balakirsky, *On the secrecy of a common knowledge created by correlated observations and transmission over helping channels*, Proceedings Workshop on Concepts in Information Theory, October 6–8, 2004, 79–92.
- V.B. Balakirsky, *Generating functions associated with random binary sequences consisting of runs of lengths 1 and 2*, Proceedings International Conference on Sequences and their Applications, October 24–28, 2004, 143–147.
- V.B. Balakirsky and L. Tolhuizen, *Guessing computed a posteriori probability distributions in a 2-state hidden Markov process*, Proceedings Workshop on Concepts in Information Theory, October 6–8, 2004, 101–109.
- V.B. Balakirsky and A.J.H. Vinck, *Asynchronous data transmission over parallel channels with dependent noise: some variations on Jack Wolf's topics*, Proceedings Workshop on concepts in Information Theory, October 6–8, 2004, 110–119.
- V.B. Balakirsky and A.J.H. Vinck, *Estimates of the decoding error probability for parallel channels with dependent noise*, Proceedings International Symposium on Information Theory and Applications (ISITA 2004), October 10–13, 2004, ISBN 4-902087-08-1, 2004, 1568–1573.
- V.B. Balakirsky and A.J. Han Vinck, *Achievable rates and decoding error probability for parallel channels with dependent noise and restricted number of users*, IEEE ISIT 2004, Chicago, June 27–July 2, 2004, ISBN 0-7803-8280-3, p. 480.
- V.B. Balakirsky and A.J. Han Vinck, *Estimates of the decoding error probability for parallel channels with dependent noise*, ISITA2004, October 10–13, 2004, Parma, Italy, ISBN 0-471-98277-6.

- V. Balakirsky and A.J. Han Vinck, *Asynchronous data transmission over parallel channels with dependent noise*, AEW4, Viareggio, October 6-8, 2004, ISBN: 3-9807929-5-1.
- J.W.M. Bergmans, S.J.M.L. van Beneden, M. Ciacci, W.M.J. Coene, A.H.J. Immink and J. Riani, *Improved correlation receiver for frame synchronization*, Proceedings International Symposium on Information Theory in the Benelux, June 2-4, 2004, ISBN 90-71048-20-9, 2004, 65-72.
- A. Braeken, S.I. Nikova and V.S. Nikov, *On cheating immune secret sharing*, In: G.R. Pellikaan (ed.), Proceedings of the 25th Symposium on Information Theory in the Benelux (Kerkrade, The Netherlands, June 2-4, 2004), Werkgemeenschap voor Informatica- en Communicatietheorie, Eindhoven, 113-120.
- A. Braeken, V.S. Nikov, S.I. Nikova, *Zigzag functions and related objects in new metric*, In: O. Geil and L.D. Andersen (eds.), Proceedings of the 8th Nordic Combinatorial Conference (Aalborg, Denmark, October 20-22, 2004), Aalborg University, Denmark, 45-58.
- A. Braeken, V.S. Nikov, S.I. Nikova and B. Preneel, *On Boolean functions with generalized cryptographic properties*, In: A. Cantaut and K. Viswanathan (eds.), Progress in Cryptology - INDOCRYPT 2004, Proceedings 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, LNCS 3348, Springer Verlag, Berlin, 120-135.
- H.J. Broersma, F.V. Fomin and G.J. Woeginger, *Parallel knock-out schemes in networks*, In: Proceedings of the 29th International Symposium on Mathematical Foundations of Computer Science (MFCS'2004), Prague, Czech Republic, August 22-27, 2004, J. Fiala, V. Koubek and J. Kratochvil (eds.), Lecture Notes in Computer Science, 3153, Springer Verlag, Berlin, 2004, ISBN 3-540-22823-3, 204-214.
- H.J. Broersma, J.L. Hurink, D. Paulusma, G.J.M. Smit, L.T. Smit and P.T. Wolkotte, *Run-time assignment of tasks to multiple heterogeneous processors*, In: Proceedings of the Progress 2004 Embedded Systems Symposium, Nieuwegein, the Netherlands, 2004, ISBN 90-73461-41-3, 185-192.
- H.J. Broersma, J.L. Hurink, D. Paulusma, G.J.M. Smit, L.T. Smit and P.T. Wolkotte, *Run-time mapping of applications to a heterogeneous re-configurable tiled system on chip architecture*, In: Proceedings of the International Conference on Field-Programmable Technology, (FPT 2004), 2004, ISBN 0-7803-8651-5, 421-424.
- H.J. Broersma and A.N.M. Salman, *The Ramsey numbers of paths versus k-pases*, In: Scientific Program of CTW04 Workshop on Graphs and Combinatorial Optimization, L. Liberti and F. Maffioli (eds.), 2004, 218-222.
- H.J. Broersma, D. Paulusma, G.J.M. Smit, F. Vlaardingerbroek and G.J. Woeginger, *The computational complexity of the minimum weight processor assignment problem*, In: J. Hromkovic, M. Nagl and B. Westfechtel (eds.) Proceedings of the 30th Workshop on Graph-Theoretic Concepts in Computer Science (WG'2004), Bad Honnef, Germany, June 21-23, 2004, LNCS 3353, Springer Verlag, ISBN 3-540-24132-9, 189-200.
- A.E. Brouwer, *On the connectivity of distance-regular graphs*, In: Proceedings Com2MaC Workshop on Distance-Regular Graphs and Finite Geometries, Busan, Korea, July 24-26, 2004.

- Ph. Bulens, G. Meurice de Dormale and J.-J. Quisquater, *An improved Montgomery modular inversion targeted for efficient implementation of FPGA*, In: O. Diessel and J.A. Williams (eds.), International Conference on Field-Programmable Technology - FTP2004, December 2004, 441-444.
- M. Ciet, J.-J. Quisquater and F. Sica, *On the security of certain DPA countermeasures*, In: H. van Tilborg (ed.), Proceedings of the 25th Symposium on Information Theory in the Benelux, 2004.
- E.K. Burke, T. Curtois, P. de Causmaecker, G.F. Post and G. Vandenberghe, *A hybrid heuristic ordering and variable neighbourhood search for the nurse rostering problem* In: Proceedings of The 5th international conference on the Practice and Theory of Automated Timetabling, M.A. Trick, E.K. Burke (Eds.), ISBN 0-88748-413-1, 2004, 445-446.
- Ph. Cara, E. Dirckx, J. Lemeire and B. Smets, *Exploiting symmetrical properties for partitioning of models in PDES*, Proceedings of the PADS 2004 Conference, IEEE Press, 2004, 189-194.
- S. Degen, J. Verschuren and T. Veugen, *Security of fixed and wireless computer networks*, Proceedings COSIC course, Katholieke Universiteit Leuven, 2004.
- V.G. Deineko, M. Hoffmann, Y. Okamoto and G.J. Woeginger, *The traveling salesman problem with few inner points*, In: K.Y. Chwa and J.I. Munro (eds.), Proceedings of the 10th International Computing and Combinatorics Conference (COCOON'2004), Jeju Island, Korea, August 17-20, 2004, LNCS 3106, Springer Verlag, 268-277.
- A. Descampe, F.-O. Devaux, J.-D. Legat, B. Macq and G. Rouvroy, *An efficient FPGA implementation of a flexible JPEG 2000 decoder for digital cinema*, Eupisco 2004, September 2004.  
 item Y. Deswarte and J.-J. Quisquater, *Remote integrity checking*, In: S. Jajodia and L. Strous (eds.), Sixth Working Conference on Integrity and Internal Control in Information Systems (IICIS), Kluwer Academic Publishers, 2004, 1-11.
- Hans Dobbertin and Gregor Leander, *Recent results on bent functions*, SETA 04.
- Jean-Paul Doignon and Jean-Claude Falmagne, *What can we learn from the transitivity parts of a relation?*, Annales du Lamsade 3, 2004, 101-113.
- H. Dreger, A. Feldmann, A. Rupp and R. Sommer, *Packet trace manipulation framework for test labs*, IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, 2004.
- V. Fack, S. Topalova, J. Winne, *On the number of reducible 2-(21,5,2) designs*, Proceedings of the Annual Workshop on Coding Theory and Applications, Bankya, Bulgaria, 2004.
- Hendrik Ferreira, Alina Hasbi, Theo Swarts and A.J. Han Vinck, *On coded M-ary frequency shift keying*, March 31 - April 2, 2004, Zaragoza, Spain, ISBN 96214-22-2, 175-179.
- F.V. Fomin, D. Kratsch and G.J. Woeginger, *Exact (exponential) algorithms for the dominating set problem*, In: J. Hromkovic, M. Nagl and B. Westfechtel (eds.), Graph-Theoretic Concepts in Computer Science

- (Proceedings 30th International Workshop, WG 2004, Bad Honnef, Germany, June 21–23, 2004), LNCS 3353, Springer-Verlag, Berlin, 2004, 245–256.
- F.-W. Fu, Y. Luo, C. Mitrpant and A.J. Han Vinck, *A generalization of MDS codes*, IEEE ISIT 2004, Chicago, June 27-July 2, 2004, ISBN 0-7803-8280-3, p. 525.
  - B. Gelbord, S. Heikkinen and H. Tschofenig, *Network attachment and address configuration using HIP*, Proceedings Workshop on HIP and Related Architectures, Washington DC, November 6, 2004.
  - A.M.H. Gerards and A. Marchetti-Spaccamela, *Preface*, In: Proceedings ATMOS Workshop 2003, Budapest, Hungary, September 15–20, 2003, Electronic notes in theoretical computer science, 92, 2004, 1–2.
  - J. Groszschaedl, S. Kumar and C. Paar, *Architectural support for arithmetic in optimal extension fields*, IEEE 15th International Conference on Application-specific Systems, Architectures and Processors (ASAP) 2004, Galveston, Texas, September 27-29, 2004.
  - L. Haryanto and A.J. van Zanten, *Snake-in-the-box codes and Euclidean geometries*, Proceedings of the Ninth International Workshop ACCT, June 2004, Kranevo, Bulgaria, 208–213.
  - I. Hassoune, J.-D. Legat, F. Macé, J.-J. Quisquater and F.-X. Standaert, *A dynamic correct mode logic to counteract power analysis attacks*, DCIS 2004 - 19th Conference on Design of Circuits and Integrated Systems, November 2004, 186–191.
  - P.J.M. Havinga and J.L. Hurink and T. Nieberg, *Size-controlled dynamic clustering in mobile wireless sensor networks*, In: Proceedings of the SCS Western Multi-Conference, Workshop on Computer Networks and Distributed Systems, (CNDS04), 2004.
  - S. Heitmann, J.L. Hurink and T. Nieberg, *Job-Shop scheduling with buffers*, In: Proceedings of the Ninth International Workshop on Project Management and Scheduling, 2004, 238–241.
  - C. Hoede, X. Liu and L. Zhang, *Information extraction based on knowledge graph theory*, In: Proceedings of the 12th International Conference on Concepts Structures, D. Pfeiffer, K.E. Wolff and S. Delugach (eds.), Huntsville, Alabama, USA, 2004, ISBN 3-8322-2950-7, 43–54.
  - C. Hoede, X. Liu, L. Zhang, *Extracting causal relationships from written text*, In: Proceedings of the 12th International Conference on Concepts Structures, D. Pfeiffer, K.E. Wolff and H.S. Delugach (eds.), Huntsville, Alabama, USA, 2004, ISBN 3-8322-2950-7, 115–128.
  - W. van Hove, *A hyper-arc consistency algorithm for the soft alldifferent constraint*, in: M. Wallace (ed.), Proceedings of the Tenth International Conference on Principles and Practice of Constraint Programming (CP 2004), LNCS 3258, Springer, 2004, 679–689.
  - J.L. Hurink and T. Nieberg, *Wireless communication graphs*, In: Proceedings of DEST International Workshop on Signal Processing for Sensor Networks, Intelligent Sensors, Sensor Networks & Information Processing Conference, Melbourne, Australia, 2004, ISBN 0-7803-8894-1, 367–372.

- J.L. Hurink and T. Nieberg, *Local, distributed topology control for large-scale wireless ad-hoc networks*, In: Proceedings of the International Workshop on Wireless Ad-Hoc Networks (IWVAN'04), Oulu, Finland: Centre for Wireless Communications, 2004.
- J.L. Hurink, W. Kern and T. Nieberg, *A robust PTAS for maximum independent sets in unit disk graphs*, In: Proceedings of the 30th workshop on Graph Theoretic Concepts in Computer Science, J. Hromkovic, M. Nagl and B. Westfechtel (eds.), Lecture Notes in Computer Science, 3353, Bad Honnef, Germany, Springer Verlag, 2004, ISBN 3-540-24132-9, 214–221.
- J.L. Hurink, G.K. Rauwerda, G.J.M. Smit and L.T. Smit, *BER estimation for HiperLAN/2*, In: Personal Wireless Communications, I.G. Niemegeers and S.M. Heemstra-deGroot (eds.), Lecture Notes in Computer Science, 3260, Springer Verlag, 2004, ISBN 3-540-23162-5, 164–179.
- J.L. Hurink, G.J.M. Smit and L.J. Smit, *Run-time adaptation of a reconfigurable mobile UMTS receiver*, In: Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms, CSREA Press, 2004, ISBN 1-932415-42-4, p. 13.
- K.A.S. Immink and C. Kui, *On the size of a type of RLL codes*, WIC Symposium on Information Theory, Rolduc, May 2004, 3946.
- K.A.S. Immink and A.J. van Wijngaarden, *On guided scrambling with guaranteed maximum run-length constraints*, IEEE international symposium on information theory (ISIT), Chicago, June 2004.
- K.A.S. Immink and A.J. van Wijngaarden, *On the selection of guided scrambling sequences that provide guaranteed maximum run-length constraints*, WIC Symposium on Information Theory, Rolduc, May 2004, 25–29.
- A.A.C.M. Kalker, D. Maas and F.M.J. Willems, *Semantic lossless source coding* (invited), Proceedings 42nd Annual Allerton Conference on Communication, Control and Computing, 29, September 29 – October 1, 2004.
- A.A.C.M. Kalker, D. Maas and F.M.J. Willems, *Semantic compaction*, Proceedings workshop on concepts in information theory, October 6-8, 2004, 9–12.
- A.A.C.M. Kalker and F.M.J. Willems, *Coding theorems for reversible embedding*, (invited), Proceedings DIMACS Series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, 66, March 17–19, 2004, 61–76.
- Samir Khuller, Yoo-Ah Kim and Gerhard J. Woeginger, *Approximation schemes for broadcasting in heterogeneous networks*, Proceedings of the 7th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX'2004), LNCS 3122, Springer Verlag, 2004, 163–170.
- S. Kumar, K. Lemke and C. Paar, *Some Thoughts about implementation properties of stream ciphers*, SASC - State of the Art of Stream Ciphers Workshop, Brugge, Belgium, October 14-15, 2004.
- T. Lange, *Montgomery addition for Genus two curves*, ANTS 2004.

- T. Lange and M. Stevens, *Efficient doubling on Genus two curves over binary fields*, SAC 2004.
- Y.-G. Kim and A.J. Han Vinck, *Capacity of BPSK signaling in fading channels with generalized selection combining*, 2004 IEEE International Conference on Communications (ICC 2004), ISBN 0-7803-8534-9.
- H. Kostadinov, H. Morita and A.J. Han Vinck, *On soft decoding of coded QAM using integer codes*, ISITA2004, Parma, Italy, October 10-13, 2004, ISBN 0-471-98277-6.
- F. Lefébre, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *Reconfigurable hardware solutions for the digital rights management of digital cinema*, DRM2004, ACM, 2004, 40–53.
- J.-D. Legat, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *Compact and efficient encryption/decryption module for FPGA implementation of AES Rijndael very well suited for small embedded A*, ITCC2004, special session on embedded cryptographic hardware, IEEE Computer Society, vol. II, April 2004, 583–587.
- F. Lefébre, J.-D. Legat, B. Macq, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *Hardware implementation of a fingerprinting algorithm suited for digital cinema*, Eupisco 2004, September 2004.
- A.K. Lenstra and T. Voss, *Automated IS risk assessment and aggregation*, In: Proceedings 13th annual RSA conference, San Francisco, February 23–27, 2004.
- A.K. Lenstra and T. Voss, *Information security risk assessment, aggregation, and mitigation*, In: H. Wang, J. Pieprzyk and V. Varadharajan (eds.), Information Security and Privacy (Proceedings 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13–15, 2004, LNCS 3108, Springer-Verlag, Berlin, 2004, 391–401.
- Asaf Levin and Gerhard J. Woeginger, *The constrained minimum weighted sum of job completion times problem*, In: L. D. Bienstock and G. Nemhauser (eds.), Proceedings of the 10th Conference on Integer Programming and Combinatorial Optimization (IPCO'2004), New York, USA, June 7–11, 2004, LNCS 3064, Springer Verlag, 2004, 298–307.
- Y. Luo, C. Mitrpant and A.J. Han Vinck, *Achieving the perfect secrecy for the Gaussian wiretap channel with side information*, IEEE ISIT 2004, Chicago, June 27–July 2, 2004, ISBN 0-7803-8280-3, p. 47.
- A. Martinez and F.M.J. Willems, *Fundamental limits on non-linear receivers in optical fibre systems*, Proceedings 25th symposium on Information Theory in the Benelux, June 2–4, 2004, Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, 2004, 57–64.
- V.S. Nikov, S.I. Nikova and B. Preneel, *Robust metering schemes for general access structures*, In: J. López, S. Qing and E. Okamoto (eds.), Information and Communications Security, Proceedings 6th International Conference, ICICS 2004, Malaga, Spain, October 27–29, 2004, LNCS 3269, Springer-Verlag, Berlin, 2004, 53–65.
- G.R. Pellikaan (ed.), Proceedings of the 25-th Symposium on Information Theory in the Benelux, Kerkrade, The Netherlands, June 2-4, 2004, 264 pages.

- L. Perret, *A geometrical approach to a polynomial equivalence problem*, Proceedings of the International Conference on Polynomial System Solving (ICPSS), in honour of Daniel Lazard, 2004, 30–33.
- G. Piret, J.-J. Quisquater, G. Rouvroy and F.-X. Standaert, *On the security of the DeKart primitive*, In: J.-J. Quisquater, P. Paradinas and Y. Deswarte (eds.), Smart Card Research and Advanced Applications (CARDIS 2004), Kluwer Academic Publishers, August 2004, 241–254.
- K.R. Pruhs and G.J. Woeginger, *Approximation schemes for a class of subset selection problems*, In: M. Farach-Colton (ed.), Proceedings of the 6th Latin American Conference on Theoretical Informatics (LATIN'2004), Buenos Aires, Argentina, April 5-8, 2004, LNCS 2976, Springer Verlag, 2004, 203–211.
- K.R. Pruhs, P. Uthaisombut and G.J. Woeginger, *Getting the best response for your Erg*, In: T. Hagerup and J. Katajainen (eds.), Proceedings of the 9th Scandinavian Workshop on Algorithm Theory (SWAT'2004), Humlebaek, Denmark, July 8–10, 2004, LNCS 3111, Springer Verlag, 2004, 14–25.
- G.F. Post and B. Veltman, *Harmonious personnel scheduling*, In: Proceedings of The 5th international conference on the Practice and Theory of Automated Timetabling, M.A. Trick and E.K. Burke (eds.), 2004, ISBN 0-88748-413-1, 557–559.
- L.A.M. Schoenmakers and P.T. Tuyls, *Practical two-party computation based on the conditional gate*, In: P.J. Lee (ed.), Advances in Cryptology - ASIACRYPT 2004, Proceedings 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5–9, 2004, LNCS 3329, Springer-Verlag, Berlin, 2004, 119–136.
- L.A.M. Schoenmakers and P.T. Tuyls, *Secure computation based on the conditional gate*, Proceedings Workshop on Secure Multiparty Protocols, SMP 2004, Amsterdam, October 7–8, 2004.
- L.A.M. Schoenmakers and P.T. Tuyls, *Private profile matching*, In: W. Verhaegh, E. Aarts and J. Korst (eds.), Proceedings of the 2nd Philips Symposium on Intelligent Algorithms (SOIA'04), Eindhoven, 2004, Technical Note TN-2004/01016, Philips Research Laboratories, Eindhoven, 149–160.
- G.J. Still, *Approximation and optimization: classical results and new developments*, In: Proceedings of PARAOPT VII, in 'Aportaciones Matematicas', J. Guddat (ed.), Societa Matematica Mexicana, 2004, ISBN 968-36-7074-1, 207–233.
- L. Stougie, *Polynomial solvability of Mader's edge-disjoint paths problem (Abstract)*, Proceedings Workshop on Graphs and Combinatorial Optimization (CTW04), Como, Italy, May 31–June 2, 2004, Electronic Notes in Theoretical Computer Science, 17, 2005, page 7.
- INengah Suparta and A.J. van Zanten, *On a class of Gray codes with maximum crossover Hamming distance*, Proceedings of the Ninth International Workshop ACCT, Kranevo, Bulgaria, June 2004, 362–367.
- T.J. Tjalkens, *Storage complexity of source codes*, General Theory of Information Transfer and Combinatorics, Universität Bielefeld, Germany, April 26–30, 2004, p. 1.

- T.J. Tjalkens, *A comparative complexity study of fixed-to-variable length and variable-to-fixed length source codes*, Proceedings of the Twenty-fifth symposium on Information Theory in the Benelux, June 2–4, 2004, G.R. Pelikaan (ed.), Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, 2004, 81–88.
- T.J. Tjalkens and F.M.J. Willems, *Source coding, Information Theory in the Benelux: An overview of WIC Symposia 1980-2003*, Werkgemeenschap voor Informatie- en Communicatietheorie, Enschede, 2004, 41–60.
- V. Vavrek and A.J. van Zanten, *Negacyclic conference matrices and cyclic codes with parameters  $(n=4t, w=2t-1, d=2t)$* , Proceedings of the Ninth International Workshop ACCT, Kranevo, Bulgaria, June 2004, 390–395.
- A.J. Han Vinck, *Proceedings of the Workshop on Concepts in Information Theory*, October 6–8, 2004, Viareggio, ISBN 3-9807929-5-1.
- F.M.J. Willems, *Computation of the Wyner-Ziv rate distortion function*, General Theory of Information Transfer and Combinatorics, April 26–30, 2004, Universität Bielefeld, Bielefeld, Germany, 2004, p. 1.
- Gerhard J. Woeginger, *Space and time complexity of exact algorithms: Some open problems*, In: R. Downey, M. Fellows and F. Dehne (eds.), Proceedings of the 1st International Workshop on Parameterized and Exact Computation (IWPEC'2004), Bergen, Norway, September 14–17, 2004, LNCS 3162, Springer Verlag, Berlin, 2004, 281–290.

#### 4.6 Preprints and Internal Reports

- K. Aardal and F. Eisenbrand, *Integer programming, lattices, and results in fixed dimension*, CWI report PNA-E0421, 2004.
- A. Braeken, V.S. Nikova and S.I. Nikova, *On cheating immune secret sharing*, Cryptology ePrint ARchive nr. 2004/200.
- A. Braeken, V.S. Nikov, S.I. Nikova and B. Preneel, *On Boolean functions with generalized cryptographic properties*, Cryptology ePrint Archive nr. 2004/259).
- H.J. Broersma and A.N.M. Salman, *On Ramsey numbers for paths versus wheels*, Memorandum afdeling TW, no. 1742, Universiteit Twente, 2004, 12 pages.
- H.J. Broersma and A.N.M. Salman, *Path-kipas Ramsey numbers*, Memorandum afdeling TW, no. 1743, Universiteit Twente, 2004, 11 pages.
- P. Brucker, S. Heitmann, J.L. Hurink and T. Nieberg, *Job-shop scheduling with limited capacity buffers*, Osnabrücker Schriften zur Mathematik, Reihe P, 253, 2004.
- T. Brueggemann and W. Kern, *An improved local search algorithm for 3-SAT*, Memorandum Afdeling TW, no. 1709, Universiteit Twente, 2004, 14 pages.
- F. J. van de Bult, D.C. Gijswijt, J.P. Linderman, N.J.A. Sloane and A.R. Wilks, *A slow-growing sequence defined by an unusual recurrence*, preprint, 2004.

- M. Chudnovski, J. Geelen, B. Gerards, L. Goddyn, M. Lohman and P. Seymour, *Packing non-zero  $a$ -paths in group-labeled graphs*, preprint, 2004.
- Arjeh Cohen, Hans Cuypers, Dorina Jibeteau and Mark Spanbroek, *Exercise language*, LeActiveMath Deliverable, December 2004.
- P.-J. Fioole, L. Kroon, G. Maròti and A. Schrijver, *A rolling stock circulation model for combining and splitting of passenger trains*, CWI report PNA-E0420, 2004.
- H. Fleuren, M.G.C. van Krieken and R. Peeters, *A Lagrangean relaxation based algorithm for solving set partitioning problems*, Center Discussion Paper 2004-44.
- M. Freedman, L. Lovász and A. Schrijver, *Graph parameters and reflection positivity*, Oberwolfach Reports, 1, 2004, 79–81.
- J.F. Geelen, A.M.H. Gerards, L. Goddyn, B. Reed, P. Seymour and A. Vetta, *The odd case of Hadwiger's conjecture*, preprint, 2004.
- J.F. Geelen, A.M.H. Gerards and G. Whittle, *On Rota's conjecture and excluded minors containing large projective geometries*, preprint, 2004.
- J.F. Geelen, A.M.H. Gerards and G. Whittle, *Tangles, tree-decompositions, and grids in matroids*, Technical Report Research Report 04-5, School of Mathematical and Computing Sciences, Victoria University, Wellington, New Zealand, 2004.
- B. Gelbord et al. *Algorithms and parameters for Electronic Signatures*, ETSI Specialist Task Force 263 Deliverable TS 102 176, ETSI Electronic Signatures and Infrastructures (ESI), 2004
- B. Gelbord et al. *Ambient networks intermediate security architecture*, Ambient Networks FP6 Deliverable D7.1, 2004, [http://www.ambient-networks.org/publications/D7-1\\_PU.pdf](http://www.ambient-networks.org/publications/D7-1_PU.pdf).
- B. Gelbord et al. *Security requirements, concepts, and architectural principles*, Ambient Networks FP6 Report R7.1, 2004.
- B. Gelbord et al. *Initial security requirements and concepts for secure access and mobility procedures*, Ambient Networks FP6 Report R7.2, 2004.
- D. Gijswijt and P. Moree, *A combinatorial identity arising from cobordism theory*, preprint 2004.
- D. Gijswijt, A. Schrijver and H. Tanaka, *New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming*, preprint 2004.
- N. Gvozdenović and M. Laurent, *Semidefinite bounds for the stability number of a graph via sums of squares of polynomials*, preprint 2004.
- L. Haryanto and A.J. van Zanten, *Covers of hypercubes by snakes and Euclidean geometries*, Report CS 04-03, Department of Computer Science, Universiteit Maastricht, 2004.
- C. Hoede, *Basic concepts in social sciences III*, Memorandum Afdeling TW no. 1711, Universiteit Twente, 2004, 22 pages.

- C. Hoede, *Syntax and semantics: A comparison of the structuralistic language theory of Ebeling with knowledge graph theory*, Memorandum Afdeling TW, no. 1710, Universiteit Twente, 2004, 24 pages.
- H. van der Holst, *A polynomial time algorithm to find a linkless embedding of a graph*, preprint, 2004.
- C.J.H. Hurkens, J.C.M. Keijsper, L. Stougie, *Virtual private network design: a proof of the tree routing conjecture on ring networks*, SPOR-report 2004-15, Technische Universiteit Eindhoven, 2004.
- D. Jibetean and M. Laurent, *Converging semidefinite bounds for global unconstrained polynomial optimization*, preprint, 2004.
- R. Joosten, G. Kleinhuis, J.-W. Knobbe and P. Lenoir, *About designing RGE Security functions*, 2004 ([http://www.rge.brabantbreedband.nl/docs/RGE\\_D5.3.pdf](http://www.rge.brabantbreedband.nl/docs/RGE_D5.3.pdf)).
- E. de Klerk, M. Laurent, P. Parrilo, *A ptas for the minimization of polynomials of fixed degree over the simplex*, preprint, 2004.
- L. Kroon and G. Maróti, *Maintenance routing for train units: the scenario model*, CWI report PNA-E0414, 2004.
- L.G. Kroon and G. Maróti, *Maintenance routing for train units: the transition model*, CWI-report PNA-E0415, 2004.
- R. Lachman, E. Martis and T. Veugen, *Beveiliging van webdiensten*, TNO-report 33265, March 11, 2004.
- M. Laurent, *Revisiting two theorems of Curto and Fialkow on moment matrices*, preprint 2004.
- T. Nieberg, *On cyclic plans for scheduling a smart card personalization system*, TR-CTIT-04, no. 01, Universiteit Twente, 2004.
- T. Nieberg and J.L. Hurink, *A PTAS for the minimum dominating set problem in unit disk graphs*, Memorandum Afdeling TW, no. 1732, Universiteit Twente, 2004, 14 pages.
- V.S. Nikov and S.I. Nikova, *New monotone span programs from old*, Cryptology ePrint Archive, nr. 2004/282.
- R. Pellikaan and X.-W. Wu, *Codes and cryptography on algebraic curves*, Working title of a book to appear at Cambridge University.
- G.F. Post and H.W.A. Ruizenaar, *Clusterschemes in Dutch secondary schools*, Memorandum Afdeling TW, no. 1707, Universiteit Twente, 2004, 13 pages.
- A. Schrijver, *Polyhedral combinatorics and combinatorial optimization*, Journée Annuelle — Recherche Opérationnelle, Société Mathématique de France, Paris, 2004, 59–74, 2004.
- INengah Suparta and A.J. van Zanten, *Ternary self-orthogonal greedy codes*, Report CS 04-01, Department of Computer Science, Universiteit Maastricht, 2004.
- V. Vavrek and A.J. van Zanten, *Generating functions for finite fields and their applications to Paley type conference matrices I*, Report CS 04-02, Department of Computer Science, Universiteit Maastricht, 2004.

- V. Vavrek and A.J. van Zanten, *Generating functions for finite fields and their applications to Paley type conference matrices II*, Report CS 04-04, Department of Computer Science, Universiteit Maastricht, 2004.

## 4.7 Patents

- S.K. Ahn, K.A.S. Immink, H.T. Kim and S.W. Suh, *Apparatus of Converting a series of data words into modulated signals*, US Patent 6,829,306, December 2004.
- M.E. van Dijk, P.T. Tuyls and L.A.M. Schoenmakers, *Method and system for generating a common secret key*, (priority date 20-09-2002/international filing date 11-08-2003/international publication date 01-04-2004), no WO2004028075.
- G. van den Enden, K.A.S. Immink, J.A.H. Kahlman, T. Nakagawa, K. Nakamura T. Narahara and Y. Shimpuku, *Modulation apparatus/method, demodulation apparatus/method and program presenting medium*, US Patent 6,677,866, January 2004.
- A. Gorokhov and F.M.J. Willems, *Transmission system*, WO 2004/030264, April 8, 2004.
- K.A.S. Immink, *Method and apparatus of converting a series of m-bit information words into a modulated signal*, US Patent 6,768,432, July 2004.
- K.A.S. Immink, C. Van Uijen and H.W. Wong-Lam, *Modulation code system and methods for encoding and decoding a signal by multiple integration*, US Patent 6,809,662, October 2004.
- A.A.C.M. Kalker and F.M.J. Willems, *Lossless data embedding*, WO 2004/066297 August 8, 2004.
- A.A.C.M. Kalker and F.M.J. Willems, *Encoding and decoding a media signal*, WO 2004/032520, April 15, 2004.
- Berry Schoenmakers, Pim Tuyls and Evgeny Verbitskiy, *Approximate matching of biometric templates under the encryption*, patent application, March 2004.

## 5 Lectures in 2004

- K. Aardal
  - *Frequency assignment and combinatorial optimization: selected topics*, Department of Informatics, Bergen University, September 13, 2004.
- C. Archer
  - *Algorithms for isomorphisms of group extensions*, University of Warwick, March 15, 2004.
  - *The Frattini subgroup and RWPri geometries*, International workshop on Groups, Algebras and Geometries, Alden-Biesen, August 28, 2004.
  - *Linear equations for group extensions*, EIDMA Symposium, Mierlo, November 25, 2004.
- J. De Beule
  - *The smallest sets of points meeting all generators of  $H(2n, q^2)$* , Workshop Blocking sets in finite geometry, Napels, Italy, February 23 - 27, 2004.
  - *The smallest sets of points meeting all generators of  $Q(2n, q)$ ,  $q \geq 3$ ,  $q$  prime*, Seminar finite geometry, Potenza, Italy, March 1–2, 2004.
  - *Minimal blocking sets of size  $q^2 + 2$  of  $Q(4, q)$ ,  $q$  an odd prime, do not exist*, Incidence Geometry, International conference, La Roche, Belgium, May 23–29, 2004.
  - *The Hermitian variety  $H(5, 4)$  has no ovoids*, EIDMA-Symposium 2004, Mierlo, The Netherlands, November 25–26, 2004.
- P.S. Bonsma
  - *Spanning trees with many leaves in graphs with minimum degree 3*, EIDMA Symposium, Mierlo, The Netherlands, November 26, 2004.
- N. Bougard
  - *Orbits on vertices and edges in finite regular graphs*, EIDMA 2004 Symposium, November 25, 2004.
- G. Brinkmann
  - *Generating benzenoids and fusenes with perfect matchings*, DIMACS-GERAD Workshop Computers and Discovery, Montreal, Canada, May 2004.
- J.J.J. van den Broek
  - *Capacity test for shunting movements*, Algorithmic Methods for Railway Optimization, Dagstuhl, Germany, June 2004.
- H.J. Broersma
  - *Parallel knock-out schemes in networks*, International Conference on Mathematical Foundations in Computer Science (MFCS'04), Prague, Czech Republic, August 23, 2004.
  - *Knock-out numbers of graphs*, Theory Seminar, University of Durham, Durham, U.K., October 29, 2004.

- A.E. Brouwer
  - *Uniqueness of the Patterson graph*, Busan, Korea, Com<sup>2</sup>MaC Conference on Association Schemes, Codes and Designs, 2004.
- T. Brueggemann
  - *An improved deterministic local search algorithm for 3-SAT*, Cologne Twente Workshop (CTW2004) on Graphs and Combinatorial Optimization 2004, Lovenno di Menaggio, Italy, June 1, 2004.
  - *Two exponential neighborhoods for single-machine scheduling with release dates to minimize total completion time*, Project Management and Scheduling (PMS), Nancy, France, April 27, 2004.
- B. De Bruyn
  - *The nonexistence of distance-regular graphs with intersection array  $\{80, 78, 76, 56; 1, 2, 12, 40\}$* , Incidence Geometry, International Conference at La Roche, La Roche, Belgium, May 24, 2004.
  - *Near polygons, a nice class of graphs*, University of Regina, Regina, Canada, August 23, 2004.
  - *Near polygons, a nice class of graphs*, Discrete Mathematics Seminar, University of Denver, Denver, USA, August 31, 2004.
- Ph. Cara
  - *Using the Frattini subgroup and independent generating sets to study RWPri geometries*, Groups and Representations Conference (dedicated to the 60th birthday of Gary Seitz), University of Oregon, Eugene, Oregon, USA, March 25, 2004.
  - *The Frattini subgroup and RWPri geometries*, International Conference on INCIDENCE GEOMETRY, La Roche, Belgium, May 24, 2004.
  - *Incidence geometry and finite groups*, University of Glasgow, UK, invited by Prof. K. Brown, June 7, 2004.
  - *On the unique independent set of size four in  $PSL(2, 31)$* , COMBINATORICS 2004, Catania, Italy, September 16, 2004.
- J. Christophe
  - *Le polytope des sous-espaces d'un espace affine fini*, Séminaire de Géométrie, combinatoire et théorie des groupes, ULB, Belgium, January 21, 2004.
  - *The polytope of the subspaces of a finite affine space*, 11th Mathematical Programming Meeting, Han-sur-Lesse, February 19, 2004.
  - *Finding facets of the polytope of subspaces of a finite affine space*, ULB - UGent Seminar on Incidence Geometry, May 14, 2004.
- M.Cimráková Cajková
  - *Clique algorithms for classifying substructures in generalized quadrangles*, CTW 2004 on Graphs and Combinatorial Optimization, Milano, Italy, May 3 1- June 2, 2004.
  - *Searching for minimal blocking sets in generalized quadrangles*, Combinatorics'04, Catania, Italy, September 12–18, 2004.

- *Searching for maximal partial ovoids and minimal blocking sets in generalized quadrangles*, EIDMA 2004 Symposium, Mierlo, The Netherlands, November 25–26, 2004.
- F. De Clerck
  - *From finite projective space to finite incidence geometry. Some case studies*, University College Dublin (Ireland), February 2004.
- A.M. Cohen
  - *Lie algebras and geometry*, Day in honour of Prof. Zara, Amiens, March 31, 2004.
  - *Computing with groups of Lie type using Lie algebras*, Conference "Lie algebras, their classifications and applications", Braunschweig, May 20, 2004.
  - *OpenMath issues arising from Algebra Interactive*, OPpenMath Workshop, Helsinki, May 21, 2004.
  - *MathDox and graph non-isomorphism*, Brouwer Colloquium, Nijmegen, November 22, 2004.
- K. Coolsaet
  - *A distance regular graph with intersection array  $(21, 16, 8; 1, 4, 14)$  does not exist*, Seminar on Incidence Geometry, Gent University, Belgium, May 7, 2004.
  - *There is a unique  $srg(105, 32, 4, 12)$* , International Conference on Incidence Geometry, Laroche, Belgium, May 23–29, 2004.
- E.R. van Dam
  - *Maximin Latin hypercube designs in two dimensions*, International Conference on Association Schemes, Codes and Designs, Pusan, Korea, July 21, 2004.
  - *Spectral characterizations of graphs*, International workshop on distance-regular graphs and finite geometry, Pusan, Korea, July 25, 2004.
  - *A new family of distance-regular graphs with unbounded diameter*, TU Eindhoven, December 15, 2004.
- J. Degraer
  - *The strongly regular subgraphs of the McLaughlin graph: a computer approach*, ULB-UGent Seminar on Incidence Geometry, Gent University, Belgium, April 30, 2004.
  - *Classification of strongly regular graphs*, SymNet Summer School 2004, University of St Andrews, St Andrews, Scotland, June 28 - July 2, 2004.
  - *The strongly regular subgraphs of the McLaughlin graph*, Combinatorics '04, Catania, Italy, September 12-18, 2004.
- A. Devillers
  - *A classification of finite partial linear spaces with a primitive rank 3 automorphism group of almost simple type or of grid type*, ULB-UGent Interuniversity Seminar on Buildings and Finite Geometry, January 23, 2004.

- *A classification of finite partial linear spaces with a primitive rank 3 automorphism group of almost simple type or of grid type*, Incidence Geometry International Conference, La Roche-en-Ardenne, May 28, 2004.
- *Partial linear spaces built from the classical generalized hexagons*, Buildings 2004, Darmstadt, Germany, October 6, 2004.
- J.-P. Doignon
  - *Le polytope des ordres totaux: nouvelles inégalités*, Séminaire Mathématiques Discrètes et Sciences Sociales, CAMS, Paris, January 12, 2004.
  - *Vertex projections of polytopes: some examples*, 11th Mathematical Programming Meeting, Han-sur-Lesse, February 19, 2004.
  - *Projection d'ordres totaux en biordres*, Programme 3ème cycle FNRS Aide à la Décision et Modélisation des Préférences, Brussels, February 21, 2004.
  - *A Variant of Turán Theorem*, ULB - UGent Seminar on Incidence Geometry, Brussels, March 5, 2004.
  - *Optimal linear inequalities for the edge and stability numbers*, 9th International Conference on Discrete Mathematics: Embedded Structures, Dortmund, August 31, 2004.
  - *What can we learn from intransitivity?*, European Mathematical Psychology Group, Ghent, September 2, 2004.
- T.S.H. Driessen
  - *A survey on the potential approach in cooperative game theory*, Game Theory Seminar, University of Technology, Wroclaw, Poland, January 27, 2004.
  - *Associated consistency and values for TU games*, Second World Congress of the Game Theory Society, Marseille, France, July 7, 2004.
  - *Convexity of production, common pool and oligopoly games*, Game Theory and Mathematical Economics, International Conference in memory of Jerzy Los (1920-1998), Warsaw, Poland, September 8, 2004.
  - *Old versus new results for one-concave TU games: characterizations and an application*, Game Theory Seminar, CentER, Tilburg, December 17, 2004.
- D. Van Dyck
  - *To be or not to be Yutsis*, CTW 2004 on Graphs and Combinatorial Optimization, Milano, Italy, May 31 - June 2, 2004.
- V. Fack
  - *Searching for ovoids and spreads in generalized quadrangles*, MSI Colloquium, Australian National University, Canberra, Australia, January 22, 2004.
  - *Searching for special substructures in combinatorial objects*, Dutch Belgian Mathematical Conference, Tilburg, Netherlands, April 16 - 17, 2004.

- *Searching for maximal partial ovoids and spreads in generalized quadrangles*, International Conference on Incidence Geometry, Laroche, Belgium, May 23 - 29, 2004.
- *Maximal partial ovoids in symplectic generalized quadrangles*, Combinatorics '04, Catania, Italy, September 12–18, 2004.
- N. De Feyter
  - *Classification of affine  $(0, 2)$ -geometries*, Seminar on Incidence Geometry, Universiteit Gent, Belgium, January 9, 2004.
  - *On  $(0, \alpha)$ -geometries fully embedded in  $\text{PG}(3, q)$  and the Klein correspondence*, Incidence Geometry, International Conference, La Roche-en-Ardenne, May 27, 2004.
- S. Fiorini
  - *Le polytope des ordres totaux: nouvelles inégalités*, Séminaire Mathématiques Discrètes et Sciences Sociales, CAMS, Paris, France, January 12, 2004.
  - *0,1/2-Cuts and the linear ordering problem: surfaces that define facets*, Séminaire du GERAD, GERAD, Montreal, Canada, February 19, 2004.
  - *How to recycle your facets*, Discrete Mathematics and Optimization Seminar, McGill, Montreal, Canada, March 1, 2004.
  - *Surfaces définissant des facettes du polytope des ordres totaux*, Séminaire de Combinatoire et d'Informatique Mathématique, UQaM, Montreal, Canada, March 26, 2004.
  - *How to recycle your facets*, Mathematical Programming Seminar, CORE (UCL), Louvain-La-Neuve, Belgium, April 27, 2004.
  - *How to recycle your facets*, Bertinoro Workshop on Combinatorial Optimization 2004, Bertinoro, Italy, May 2, 2004.
  - *Packing and covering odd cycles in planar graphs*, Optimization Seminar, Advanced Optimization Laboratory at McMaster, Hamilton (Ontario), Canada, December 6, 2004.
- B. Gelbord
  - Course Privacy and Technology, Universiteit van Amsterdam, spring semester 2004.
  - Talk at Security Seminar, LIACS, Spring 2004.
  - *ICT in business*, Privacy and Technology Course, April-May 2004.
  - KWINT Panel Discussion Digital Identity (invited panel member), The Hague, April 7, 2004.
  - LappTop Lecture, Cryptography and Security, March 9, 2004.
  - Security Issues eEurope, ECP.nl, July 19, 2004
  - DRM in eEurope, eEurope Advisory Group, October 21, 2004.
  - Cryptography and Digital Government, Universiteit Maastricht, October 14, 2004.
  - Panel on Information Society, DG Information Society, Brussels, Belgium, September 29, 2004.
- A.M.H. Gerards

- *Inequivalent representations of matroids* (invited lecture), The 2004 NZIMA Conference in Combinatorics and its Applications, Lake Taupo, New Zealand, December 12–18, 2004.
- P. Govaerts
  - *On the size of maximal partial  $t$ -spreads*, ULB-UGent-VUB seminar, Ghent, Belgium, February 20, 2004.
  - *Small maximal partial  $t$ -spreads*, International Conference on Incidence Geometry, La Roche-en-Ardennes, Belgium, May 25, 2004.
  - *Cameron-Liebler line classes in  $PG(3,4)$* , Combinatorics 2004, Acireale (Capomulini), Italy, September 16, 2004.
- D. Gijswijt
  - *On a packet scheduling problem for smart antennas and polyhedra defined by circular-ones matrices*, Cologne-Twente Workshop on Graphs and Combinatorial Optimization, May 29 - June 1, 2004.
- W.H. Haemers
  - *Perfect matchings and eigenvalues*, Acireale, Italy, September 14, 2004.
  - *Which graphs are determined by their spectrum*, Magdeburg, May 4, 2004.
- F. Haot
  - *The half-3-Moufang property for generalized quadrangles*, Incidence Geometry, La Roche, May 29, 2004.
  - *On the uniqueness of the unipotent subgroups of Moufang sets*, Buildings 2004, Darmstadt, October 7, 2004.
- W.J. van Hoeve
  - *a hyper-arc consistency algorithm for the soft alldifferent constraint* (plenary lecture), Optimizations Days, Montreal, Canada, May 10–12, 2004.
  - *Exploiting semidefinite relaxations in constraint programming* (plenary lecture), CORS/INFORMS joint international conference, Banff, Canada, May 15–19, 2004.
  - *Postponing branching decisions* (poster presentation), 16th European Conference on Artificial Intelligence (ECAI 2004), Valencia, Spain, August 22–27, 2004.
  - *On global warming (softening global constraints)* (plenary lecture), 6th International Workshop on Preferences and Soft Constraints, Toronto, Canada, September 27, 2004.
  - *a hyper-arc consistency algorithm for the soft alldifferent constraint* (plenary lecture), International Conference on Principles and Practice of Constraint Programming (CP'04), Toronto, Canada, September 27 - October 01, 2004.
  - *Operations research techniques in constraint programming*, Paragon Decision Technology, Haarlem, September 21, 2004.
  - *Postponing branching decisions*, University of Nantes, France, February 19, 2004.

- J.L. Hurink
  - *Modeling of capacitated transportation systems for integral scheduling*, 9th International Workshop on Project Management and Scheduling, Nancy, France, April 27, 2004.
  - *Sequencing and scheduling*, Socrates LP Transportation and Scheduling in Telecommunication: Supply chain organization, Angers, France, September 14, 2004.
  - *Sequencing and scheduling*, ISE Graduate Seminar Series, Ohio State University, USA, October 22, 2004.
  - *Modeling of capacitated transportation systems for integral scheduling*, INFORMS Annual Meeting 2004, Denver, USA, October 26, 2004.
- D. Jibetean
  - *Global minimization of a polynomial using algebraic matrix methods*, Louvain-la-Neuve, March 23, 2004.
- E. Jochemsz
  - *Cryptanalysis of RSA using lattices*, EIDMA Seminar Combinatorial Theory, Eindhoven, March 17, 2004.
  - *Partial key exposure attacks on the RSA cryptosystem*, EIDMA PhD Symposium, Mierlo, November 26, 2004.
  - *Partial key exposure attacks on the RSA Cryptosystem*, SAFE-NL Workshop, Eindhoven, December 2, 2004.
- J. Keijsper
  - *Virtual private network design: a proof of the Tree Routing Conjecture for circuit networks*, Seminar Combinatorics and Optimization, CWI Amsterdam, February 13, 2004.
  - *Book of A. Schrijver, chapter 13: Path and flow polyhedra and total unimodularity*, TU Eindhoven, June 2, 2004.
- T. Lange
  - *Algorithms and Number Theory*, Dagstuhl Wartacrypt, Bedlewo, Polen, 2004.
  - *Number Theoretic Algorithms and their Applications*, Strobl, Austria, 2004.
  - *Finite Fields: Theory and Applications*, Oberwolfach, Germany, 2004.
  - *Seminar on zeta functions*, Technical University Tokyo, 2004.
- M. Laurent
  - *Revisiting two theorems of Curto and Fialkow on moment matrices* (invited lecture), Combinatorics, Mathematisches Forschungsinstitut Oberwolfach, January 4–10, 2004.
  - *Moment matrices, radical ideals and optimization* (invited lecture), Algorithmic, Combinatorial and Applicable Real Algebraic Geometry, MSRI, Berkely, April 12–16, 2004.

- *Moment matrices, radical ideals and optimization*, Algorithmic, Combinatorial and Applicable Real Algebraic Geometry, Mathematical Sciences Research Institute (MSRI), Berkeley, April 12–16, 2004.
- *A PTAS for minimizing polynomials of fixed degree on the simplex*, Approximations Algorithms for NP-hard Problems, Oberwolfach, June 6–12, 2004.
- D. Leemans
  - *An algorithmic analysis of the intersection property*, Seminar UG-ULB on finite geometries, Universiteit Ghent, Belgium, April 30, 2004.
  - *La vie d'un chercheur en mathématique*, Haute École Galilee, May 12, 2004.
  - *A generalization of a geometric construction due to Van Nypelseer*, EIDMA Symposium 2004, Mierlo, November 25–26, 2004.
- A.K. Lenstra  
among others:
  - talk at Lucent technologies.
  - 2 invited lectures at ACISP 2004.
  - 3 lectures in Melbourne at several workshops.
- D. Luyckx
  - *Complete caps of  $H(3, q^2)$* , Incidence Geometry – International Conference at La Roche-en-Ardenne, Belgium, May 23–29, 2004.
  - *Maximal partial spreads of  $H(2n+1, q^2)$* , Combinatorics 2004, Capomulini, Catania, Italy, September 12–18, 2004.
- H. Van Maldeghem
  - *Remarkable embeddings of remarkable geometries*, Darmstadt, Germany, January 29, 2004.
  - *Combinatorial building theory*, Conference Buildings and curvature, Oberwolfach, Germany, May 14, 2004.
  - *Small hexagons and small groups*, Würzburg, Workshop Buildings and Groups, June 9, 2004.
  - *Small quadrangles with great properties*, Stuttgart, July 14, 2004.
  - *Codes from generalized hexagons*, Com<sup>2</sup>Mac Conference on Association Schemes, Codes and Designs, Busan, South-Korea, July 20, 2004.
  - *Embeddings of generalized polygons in finite projective spaces*, Com<sup>2</sup>Mac Workshop on Distance-Regular Graphs and Finite Geometry, Busan, South-Korea, July 25, 2004.
  - *Metric properties of buildings*, conference Finite Geometry, Groups and Computation, Pingree Park, Colorado, USA, September 8, 2004.
  - *Buildings and generalized polygons: Recent Results and Open Problems*, Conference Buildings 2004, Darmstadt, Germany, October 4, 2004.
- G. Maroti

- *Maintenance routing for passenger train units*, Algorithmic Methods for Railway Optimization, Dagstuhl, Germany, June 20–25, 2004.
- T. De Medts
  - *Split BN-pairs of rank 1 and the uniqueness of splittings*, Conference Incidence Geometry, La Roche, Belgium, May 24, 2004.
  - *Inclusions of spherical buildings of equal rank*, Workshop Buildings and Groups, Würzburg, June 10, 2004.
  - *Split BN-pairs of rank 1 arising from higher rank*, Seminar, Darmstadt, June 23, 2004.
  - *Moufang sets and Jordan algebras*, Conference Buildings 2004, Darmstadt, October 5, 2004.
- B. Mühlherr
  - *Isomorphisms of Coxeter groups*, Colloquium Charlottesville, January 15, 2004.
  - *Isomorphisms of Coxeter groups*, Colloquium for F. Zara, March 30, 2004.
  - *Buildings and Amalgams*, Dutch-Belgian Mathematical Conference, April 16, 2004.
  - *Isomorphisms of Coxeter groups*, Conference on geometric group theory, Bedlewo, April 20, 2004.
  - *The isomorphism problem for Coxeter groups*, The Coxeter Legacy: Reflections and Projections, Toronto, May 16, 2004.
  - *Exotic Moufang buildings*, Incidence Geometry, La Roche, May 25, 2004.
  - *Groups acting on buildings*, Groups, Algebras and Geometries, Alden Biesen, August 25, 2004.
  - *Die Geometrie der Coxeter-Gruppen*, Colloquium, Darmstadt, June 4, 2004.
  - *Presentations of Borel-groups*, Buildings 2004, Darmstadt, October 7, 2004.
  - *5-day EIDMA minicourse 'Spherical Buildings and Groups of Lie Type'*, TU Eindhoven, March 8–12, 2004.
- A. Nguyen
  - *A combinatorial approach to Coxeter groups*, Buildings 2004, Darmstadt, Germany, October 6, 2004.
  - *A combinatorial approach to Coxeter groups*, EIDMA 2004 Symposium, Mierlo, November 26, 2004.
- T. Nieberg
  - *Size-controlled dynamic clustering in mobile wireless sensor networks*, Communications Networks and Distributed Systems, Modelling and Simulation Conference, San Diego, USA, January 21, 2004.
  - *Prolonging network lifetime by cross-layer optimization*, EYES Workshop, Ferrara, Italy, March 17, 2004.
  - *Job-shop scheduling with buffers*, Ninth International Workshop on Project Management and Scheduling, Nancy, France, April 27, 2004.

- *Local, distributed topology control for large-scale wireless ad-hoc networks*, International Workshop on Wireless Ad-Hoc Networks, Oulu, Finland, June 2, 2004.
  - *Communication in the EYES WSN: Tight integration of networking layers extends lifetime*, International Workshop on Wireless Ad-Hoc Networks, Oulu, Finland, June 3, 2004.
  - *A Roberts PTAS for maximum independent sets in unit disk graphs*, 30th Workshop on Graph Theoretic Concepts in Computer Science, Bad Honnef, Germany, June 22, 2004.
  - *Ad-hoc wireless sensor networks*, Sokrates IP: Supply Chain Management and Telecommunication Networks, Angers, France, October 14, 2004.
  - *Optimization problems on geometric intersection graphs*, Sokrates IP: Supply Chain Management and Telecommunication Networks, Angers, France, October 17, 2004.
  - *Job-Shop scheduling with limited capacity buffers*, INFORMS Annual Meeting, Denver, USA, October 26, 2004.
  - *Intelligent algorithms on (not so) restricted domains: Robust optimization*, IPA Herfstdagen on Intelligent Algorithms, Callantsoog, The Netherlands, November 24, 2004.
  - *Wireless communication graphs*, DEST International Workshop on Signal Processing for Sensor Networks, ISSNIP'04, Melbourne, Australia, December 17, 2004.
- C. Paar
    - *Elektronische Signaturen in der Praxis*, Enterprise Signature Day 2004, Düsseldorf, March 11, 2004.
    - *Elliptic curves and BMVs or why cars ill need embedded IT security*, WPI Cryptography Seminar, USA, August 9, 2004.
    - *Pervasive computing and the future of crypto engineering*, IBM T.J. Watson Research Center, USA, August 31, 2004.
    - *Trends in embedded security*, escar 2004, November 10-11, 2004.
  - D. Paulusma
    - *The computational complexity of the minimum weight processor assignment problem*, International Workshop on Combinatorics, Keio University, Japan, January 21, 2004.
    - *Locally constrained graph homomorphisms*, TUS Graph Theory Seminar, Tokyo University of Science, Japan, January 24, 2004.
    - *Tracing locally constrained homomorphisms*, Czech-Slovak Conference Graphs 2004, Vysne Ruzbachy, Slovakia, May 26, 2004.
    - *The computational complexity of the minimum weight processor assignment problem*, 30th International Workshop on Graph-Theoretic Concepts in Computer Science (WG2004), Bad Honnef, Germany, June 21, 2004.
  - R. Peeters
    - *Ranks, colours and eigenvalues*, Nederlands Mathematisch Congres, April 16, 2004.

- G.F. Post
  - *Harmonious Personnel Scheduling*, PATAT 2004 (The 5th international conference on the Practice and Theory of Automated Timetabling), Pittsburg, U.S.A., August 18, 2004.
- E. Postma
  - *Melikian Lie algebras*, EIDMA Seminar Combinatorial Theory, TU Eindhoven, October 27, 2004.
- A.N.M. Salman
  - *The Ramsey numbers of paths versus kipases*, Cologne Twente Workshop (CTW 2004) on Graphs and Combinatorial Optimization 2004, Loven di Menaggio, Italy, June 1, 2004.
  - *The computational complexity of lambda-backbone coloring*, EIDMA 2004 Symposium, Mierlo, The Netherlands, November 25, 2004.
- L.A.M. Schoenmakers,
  - *Modern cryptographic protocols for electronic voting*, Estonian Theory Days 2004, Koke, Estland, January 31, 2004.
  - *A (brief) comparison of cryptographic schemes for electronic voting*, Estonia E-Voting Event, Tartu, Estland, May 17, 2004.
  - *Practical secure computation based on threshold homomorphic El-Gamal*, EIDMA Cryptography Working Group, Utrecht, October 1, 2004.
  - *Secure computation based on the conditional gate*, SMP 2004, Amsterdam, October 8, 2004.
  - *Practical two-party computation based on the conditional gate*, C.I.R.M. Workshop on Cryptography, Luminy, November 9, 2004.
  - *Practical two-party computation based on the conditional gate*, Asiacrypt 2004, Jeju Island, Korea, December 6, 2004.
- A. Schrijver
  - *Graph parameters* (keynote talk), Combinatorics, Mathematisches Forschungsinstitut Oberwolfach, January 4–10, 2004.
  - *Polyhedral combinatorics and combinatorial optimization* (keynote talk), Journée Annuelle Société Mathématique de France, Paris, June 19, 2004.
  - *New code bounds with semidefinite programming* (invited lecture), 8th International Workshop on High Performance Optimization Techniques (HPOPT 2004), CWI, Amsterdam, June 23–25, 2004.
  - *History of combinatorial optimization* (keynote talk), Jahrestagung Gesellschaft für Operations Research (GOR), Tilburg, September 1–3, 2004.
- G.J. Still
  - *Optimization problems with complementarity constraints, optimality conditions, genericity and a parametric solution approach*, EUROPT Workshop, Rhodos, Greece, July 2, 2004.

- *On discretization methods in semi-infinite Programming*, EURO XII Conference, Rhodos, Greece, July 7, 2004.
  - *Semi-infinite Programming: An Introduction, I*, EURO Summer Institute (ESI 2004), Ankara, Turkey, July 10, 2004.
  - *Semi-infinite Programming: An Introduction, II*, EURO Summer Institute (ESI 2004), Ankara, Turkey, July 11, 2004.
  - *Semi-infinite Programming and related Problems*, Congreso Latino-Iberoamericano de Investigacion de Operaciones y Sistemas (CLAIO XII), Havana, Cuba, October 6, 2004.
- L. Storme
    - *On ovoids of  $Q(4, q)$ ,  $q$  prime*, Workshop Blocking sets, Naples, Italy, February 23–27, 2004.
    - *On the characterization of a particular class of minihypers*, University of Potenza, Italy, March 2004.
    - *Linear codes and finite geometries*, Third Croatian Congress of Mathematics, Split, Croatia, June 16–18, 2004.
    - *Linear codes meeting the Griesmer bound, minihypers, and geometric applications*, Combinatorics '04, Capomulini, Italy, September 13–18, 2004.
    - *Links of projective geometry to practical applications*, TU Graz, Austria, November 2004.
    - *Linear codes meeting the Griesmer bound and minihypers in finite projective spaces*, TU Vienna, Austria, November 2004.
    - *Shortened incidence matrices of  $PG(2, q)$ ,  $q$  prime*, Eötvös Loránd University, Budapest, Hungary, November 2004.
- L. Stougie
    - *A linear bound on the diameter of the transportation polytope*, Korteweg-De Vries Seminar, Universiteit van Amsterdam, January 28, 2004.
    - *The generalized 2-server problem*, EIDMA Combinatorial Optimization Seminar, CWI, Amsterdam, February 6, 2004.
    - *A linear bound on the diameter of the transportation polytope*, University of Rome "La Sapienza", Department of Computer Science, Rome, Italy, March 22, 2004.
    - *Algorithms and processes in life sciences*, Kick-off meeting BSIK-BRICKS, NWO, The Hague, April 15, 2004.
    - *The spy who loved theoretical computer science*, IFIP Workshop on Stochastic Integer Programming, Groningen, May 26, 2004.
    - *A linear programming formulation of Mader's edge disjoint paths problem*, Cologne-Twente Workshop on Graphs and Combinatorial Optimization 2004, Como, Italy, May 31, 2004.
- J.A. Thas
    - *Finite translation generalized quadrangles*, 10 lectures at the Università degli studi di Perugia, March 2004.
    - *Finite Geometries: Classical problems and recent developments*, Universität Stuttgart, June 2004.

- *Finite Geometries: Classical Problems and Recent Developments*, Main speaker at Trends in Geometry, Conference in memory of Beniamino Segre, Accademia Nazionale dei Lincei and Università “La Sapienza”, Rome, Italy, June 7–9, 2004.
  - *Finite translation generalized quadrangles, pseudo-ovals and pseudo-ovals*, Main speaker at Com<sup>2</sup>MaC Conference on Association Schemes, Codes and Designs, Pusan National University, Pusan, Korea, July 19–23, 2004.
  - *Embeddings of generalized polygons in finite projective spaces*, Main speaker at 2004 Com<sup>2</sup>MaC Workshop on Distance-Regular Graphs and Finite Geometry, Pusan National University, Pusan, Korea, July 24–26, 2004.
  - *Finite translation generalized quadrangles: old results, new results, open problems*, Conference Finite Geometries, Groups and Computation, Pingree Park Campus, Colorado State University, September 4–9, 2004.
- K. Thas
    - *Translation and 2-transitive generalized ovals*, Seminar on Incidence Geometry RUG-ULB, Brussels, Belgium, February 6, 2004.
    - *Local group actions of generalized quadrangles* (main lecture), Joint Meeting of the Belgian and Dutch Mathematical Societies, (Nederlands-Belgisch Mathematisch Congres), Universiteit Utrecht, April 16–17, 2004.
    - *Foundations of elation generalized quadrangles*, Incidence Geometry, International Conference, La Roche, Belgium, May, 23–29, 2004.
    - *Generalized quadrangles of order  $(q, q^2)$ ,  $q$  even, with a classical subGQ of order  $q$  containing the elation point are classical*, Finite Geometries, Groups and Computation, Pingree Park, Denver, USA, September 4–9, 2004.
    - *Some basic questions on elation generalized quadrangles*, Buildings 2004, Technische Universität Darmstadt, Darmstadt, Germany, October 4–7, 2004.
    - *Groups and generalized quadrangles* (invited seminar), The 2004/2005 mathematics seminar series, The University of Sussex, Brighton (UK), November 3, 2004.
    - *Elation generalized quadrangles* (invited seminar), Combinatorics Study Group, Queen Mary, University of London (UK), November 12, 2004.
  - C. Tonesi
    - *Distance-regular  $(0, \alpha)$ -reguli*, Joint UGent-ULB seminars, February 13, 2004.
    - *$(0, \alpha)$ -reguli adistanza regolare*, Seminario Matematico di Brescia, Italy, April 7, 2004.
    - *Distance-regular  $(0, \alpha)$ -reguli*, Combinatorics 2004, Acireale-Capomulini, Italy September 13–18, 2004.
  - T. Veugen
    - *Untraceable electronic cash*, Athens course, TU Delft, March 19, 2004.

- A.J. Han Vinck
  - *Permutation codes for access*, University of Dresden, May 28, 2004.
  - Several lectures on Information Theory, Sun-Yat-Sen University, Kaohsiung, Taiwan, March 2004.
- B. de Weger
  - *Partial Key Exposure Attacks on RSA*, EIDMA Cryptography Working Group, Utrecht, April 2, 2004.
  - *Cycles for the  $3n + 1$ -problem*, Dutch-Belgian Mathematical Conference, Tilburg, April 17, 2004.
  - *Internet-beveiliging*, Apeldoorn-IT congres "IT met het oog op de toekomst", Apeldoorn, October 28, 2004.
- J. Winne
  - *Construction techniques for incidence structures*, Combinatorics '04, Catania, Italy, September 12–18, 2004.
- S. De Winter
  - *On the classification of linear representations of semipartial geometries*, UGent seminar on incidence geometry, Gent, Belgium, February 26, 2004.
  - *On semi-pseudo-ovals*, ULB-UGent seminar on incidence geometry, Brussels, Belgium, May 14, 2004.
  - *Linear representations of semipartial geometries*, Incidence Geometry, La Roche, Belgium, May 23–29, 2004.
  - *Generalized quadrangles admitting a regular Abelian group*, Combinatorics 2004, Catania, Italy, September 12–18, 2004.
- A. De Wispelaere
  - *Distance-2-ovals of  $H(4)$  and two-character sets in  $PG(5, q^2)$* , ULB-UGent seminar, Ghent, March 26, 2004.
  - *Two-character sets in  $PG(5, q^2)$* , Incidence Geometry, La Roche-en-Ardenne, May 23–29, 2004.
  - *A Hölz design in the generalized hexagon  $H(q)$* , Combinatorics 2004, Catania, September 12–19, 2004.
  - *Uniqueness of the one-point extensions of a generalized hexagon of order 2*, Buildings and Polygons 2004, Darmstadt, October 4–7, 2004.
- G.J. Woeginger
  - *Exact algorithms*, International Symposium on Combinatorial Optimization (CO'2004), Lancaster, England, March 28–31, 2004. (Plenary speaker).
  - *Exact approaches to scheduling*, 9th International Conference on Project Management and Scheduling (PMS'2004), Nancy, France, April 26–28, 2004. (Plenary speaker).
  - *Space and time complexity of exact algorithms: Some open problems*, ALGO'2004, Bergen, Norway, September 14–17, 2004. (Invited speaker for IWPEC).

- *Approximation through relaxation*, Workshop “Fundamentals for Operations Management: Where disciplines meet”, Eindhoven, The Netherlands, September 27–28, 2004.
- *Three problems and one theorem*, Symposium Diskrete Mathematik 2004, Zürich, Switzerland, October 7–8, 2004. (Plenary speaker).
- *Three problems and one theorem*, Department of Computer Science, University of Southern Denmark, Odense, Denmark, November 11–12, 2004.
- A.J. van Zanten
  - *On a theorem of Kleitman and Erdos*, EIDMA Seminar Coding Theory and Cryptology, TU Eindhoven, March 19, 2004.
  - *On the construction of balanced Gray codes*, DAOR Conference, Novosibirsk, Russia, June 29, 2004.
- The group “Graphes et Optimisation Mathématique” of the ULB, gave lectures in 2004, at:
  - 8th Aussois Workshop on Combinatorial Optimization, Aussois, France, D. Huygens and M. Labbé, January 2004.
  - 11th Mathematical Programming Meeting, 3rd cycle FNRS, Han-sur-Lesse, Belgium, G. Fasbender, S. Garcia, D. Huygens and M. Labbé, February 2004.
  - Airo Winter 2004, Champoluc, Italy, M. Labbé, February 2004.
  - CO 2004, International Symposium on Combinatorial Optimization, Lancaster, United Kingdom, D. Huygens, March 2004.
  - Deuxième journée du groupe de travail en programmation mathématique, Conservatoire Nationale des Arts et Métiersm Paris, France, M. Labbé, April 2004.
  - INFORMS/CORS Meeting, Banff, Canada, M. Labbé, May 2004.
  - Triennial Symposium on Transportation Analysis, Le Gosier, France, M. Labbé, June 2004.
  - EURO XX, Rhodes, Greece, M. Labbé, July 2004.
  - TraLog - Transportation and Logistics, Molde, Norway, G. Fasbender and M. Labbé, August 2004.
  - Fundamental Computer Science FNRS Contact Group, Meeting on Constraints in Computer Science, Mons, Belgium, H. Mélot, October 2004.

## 6 External Grants in 2004

- **H.J. Broersma**, Universiteit Twente, received the following grants:
  - Rusland–Nederland NWO Samenwerkingsproject.
  - Nato Grant (with D. Bauer).
  - KNAW-EPAM grant for cooperation with ITB Bandung, Indonesia.
- **Ph. Cara**, ULB:
  - Postdoctoral grant of the Fonds voor Wetenschappelijk Onderzoek-Vlaanderen.
  - FWO-Vlaanderen: project "Threading and protein folding" (with B. Manderick, A. Nowé and T. Hamelryck), one research position for 2 years.
- **F. De Clerck**, Universiteit Gent received a research grant of the Fund for Scientific Research-Flanders (promotors: F. De Clerck, L. Storme, J.A. Thas and H. Van Maldeghem).
- **A. Devillers** ULB, received a grant of the "Fonds National de la Recherche Scientifique" in Belgium for a 2-months stay in the USA.
- **H. Dobbertin** received financial support for the following projects:
  - Analysis of the SHA-family hash functions, BSI (German Federal Agency for IT Security).
  - ECRYPT-Network of Excellence in Cryptography" ([www.ecrypt.eu.org](http://www.ecrypt.eu.org)).
- **T.S.H. Driessen**, Universiteit Twente, received a grant for the Russia-The Netherlands NWO Cooperation project (till August 1, 1004).
- **V. Fack**, Universiteit Gent, obtained grants for a visit to Australian National University (ANU), Canberra, Australi. Travel grant by FWO-Belgium (3450 euro) and accommodation paid by ANU.
- The position of **N. De Feyter** at Ghent University is financed by "Bijzonder Onderzoeksfonds" of Ghent University (since October 2001, renewed October 2003).
- **D. Luyckx**, Universiteit Gent, was appointed a fellow of the Fund for Scientific Research Flanders (Belgium) (F.W.O. – Vlaanderen), October 2003 – September 2006.
- **H. Van Maldeghem**, Universiteit Gent, received a research grant of the fund for scientific research flanders (promotors: F. De Clerck, L. Storme, J.A. Thas and H. Van Maldeghem).
- **C. Paar** received financial support for the following projects:
  - Infineon, "Security for Mobile Devices".
  - ECRYPT-Network of Excellence in Cryptography, ([www.ecrypt.eu.org](http://www.ecrypt.eu.org)).
  - Cryptographic Hardware, BSI (German Federal Agency for IT Security).
- **A Sadeghi** received financial support for the project ECRYPT-Network of Excellence in Cryptography, ([www.ecrypt.eu.org](http://www.ecrypt.eu.org)), 2004.

- **L.A.M. Schoenmakers**, TU Eindhoven:
  - Sentinels STW, two PhD positions for TUE (plus one postdoc for CWI, R. Cramer), project "Practical Approaches to Secure Computation (PASC)".
  - WBSO subsidie "toegepaste cryptografie", Senter, project WI 99010219 (for research at Philips Natlab).
- J. Schwenk received financial support for the project ECRYPT-Network of Excellence in Cryptography ([www.ecrypt.eu.org](http://www.ecrypt.eu.org)), 2004.
- **L. Storme**, Universiteit Gent, received:
  - a grant from the Technical University of Graz (Austria) to visit the geometry group of Prof.Dr. O. Röschel (November 7–9, 2004).
  - a research grant of the Fund for Scientific Research-Flanders (promoters: F. De Clerck, L. Storme, J.A. Thas and H. Van Maldeghem).
- **J.A. Thas**, Universiteit Gent, received a research grant of the Fund for Scientific Research-Flanders (promoters: F. De Clerck, L. Storme, J.A. Thas and H. Van Maldeghem).
- **K. Thas**, Universiteit Gent, was appointed a postdoctoral fellow of the Fund for Scientific Research – Flanders (Belgium) (F.W.O. – Vlaanderen), October 2002 – September 2005.
- **A.J. Han Vinck**, (University Duisburg-Essen) welcomed the following guests on external grants:
  - Dr. Vladimir Balakirsky, Data Security Association "Confident", St. Petersburg, Russia, June - August, October - December 2004.
  - Jaco Versfeld, South Africa, April - June 2004.
  - Prof. Raymond Yeung, Hongkong, May 2004.
  - Dr. Young Gil Kim, South Korea, June 2004.
  - Prof. Samwel Martirosyan, Armenian Academy of Sciences, November 2004
- The position of **J. Winne**, Universiteit Gent, has been financed by the Fund for Scientific Research Flanders (Belgium) (FWO) since October 2002.
- The position of **Stefaan De Winter** at Ghent University is financed by the Fund of Scientific Research - Flanders since October 2001.
- The position of **An De Wispelaere** at Ghent University is financed by the Fund of Scientific Research - Flanders since October 2002 and has been extended in October 2004.

## 7 Noteworthy Activities in 2004

### 7.1 Awards

- On October 23, 2004, **A.E. Brouwer** (TU/e) received an honorary doctorate from the University of Aalborg.
- **K.A. Schouhamer-Immink** received the following awards in 2004:
  - SMPTE Progress Medal, awarded by the Society of Motion Picture and Television Engineers (SMPTE), For the central role played in research and development of audio and video recording products.
  - Consumer Electronics Engineering Excellence Award, awarded by the IEEE Consumer Electronics Society.
  - Heyser Memorial lecturer, awarded by the Audio Engineering Society (AES), May 2004.
- In December 2004 **Gerhard J. Woeginger** received the ‘VICI’ award of NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek) for the project ‘Exact and parametric computation’, TU Eindhoven, Netherlands, 2005–2010.

### 7.2 Ph.D. Degrees

- **J. De Beule**,  
**Blocking sets and partial spreads in finite polar spaces**,  
Universiteit Gent, Belgium, May 18, 2004.  
Supervisor: Prof. Dr. L. Storme.  
**Abstract:**  
A finite generalized quadrangle (GQ) is an incidence structure consisting of points and lines and an incidence relation satisfying three basic axioms. A GQ is a translation generalized quadrangle if it satisfies extra symmetry conditions. All TGQs can be constructed inside a projective space. A partial spread of a TGQ is a set of mutually disjoint lines, the size of the partial spread is the number of lines it contains. A partial spread is maximal if it cannot be extended to a larger partial spread.  
We obtain an upper bound on the size of an arbitrary maximal partial spread of an arbitrary TGQ. For certain TGQs, we can improve the upper bound and construct examples with the largest possible size; hence, the upper bound cannot be improved in that case, and this result improves a result of G. Tallini on maximal partial spreads of  $Q(4, q)$ .  
In the second part, we consider blocking sets of certain finite classical polar spaces, i.e. sets of points such that every generator of the polar spaces meets the set at least once. It is well known that finite classical polar spaces of rank 2 (i.e. polar spaces containing only points and lines) are GQs, and that finite polar spaces of rank at least 3 are classical.  
We investigate geometric properties, and the main goal is the classification and a geometric characterization of the smallest minimal blocking sets. This goal is achieved for three different types of finite classical polar spaces, namely for the polar spaces  $Q(6, q)$ ,  $q \geq 32$  even,  $Q(2n, q)$ ,  $n \geq 3$   $q$  odd prime and  $\mathit{mathrm}H(2n, q^2)$ ,  $n \geq 2$ , where we classify the smallest minimal blocking sets as truncated cones with base an ovoid of the polar space in low dimension and vertex a subspace contained in the polar space.
- **S. Dewez**,  
**On the toll setting problem**,

Université Libre de Bruxelles, Belgium, June 8, 2004.  
Supervisors: Prof.Dr. M. Labbé and Prof. Ph. Vincke.

**Abstract:**

The problem of road taxation is considered. This problem consists in finding the toll on the roads belonging to the government or a private company in order to maximize the revenue. An optimal taxation policy consists in determining level of tolls low enough to favor the use of toll arcs, and high enough to get important revenues. Since there are two levels of decision, the problem is formulated as a bi-level bilinear program.

- **D. Van Dyck,**  
**Yutsis graphs and the computation of generalized recoupling coefficients,**  
Universiteit Gent, Belgium, May 19, 2004.  
Supervisor: Prof.Dr. V. Fack.
- **J. Guajardo,**  
**Arithmetic architectures for finite fields  $GF(P^m)$  with cryptographic applications,** Ruhr Universität Bochum, Germany, July 16, 2004.  
Supervisor: Prof.Dr.-Ing. C. Paar.
- **M. Quisquater,**  
**Applications of character theory and the Mobius inversion principle to the study of cryptographic properties of Boolean functions,**  
Katholieke Universiteit Leuven, Belgium, May 17, 2004.  
Supervisors: Prof. B. Preneel and Prof. J.J. Vandewalle.
- **B. Van Rompay,**  
**Analysis and design of cryptographic hash functions, MAC algorithms and block ciphers.**  
Katholieke Universiteit Leuven, Belgium, June 30, 2004.  
Supervisors: Prof. B. Preneel and Prof. J. Vandewalle.  
**Abstract:**  
This thesis is concerned with the analysis of cryptographic hash functions, MAC algorithms and block ciphers. Hash functions are versatile cryptographic building blocks, with applications such as the protection of the authenticity of information and digital signatures. The first part of this thesis gives an overview of existing hash functions and the different methods of designing these. Next, strategies for the cryptanalysis of hash functions are examined where we focus mainly on the popular algorithms based on the well-known MD4-design. The use of techniques similar to those introduced by H. Dobbertin in the mid-nineties (a combination of differential cryptanalysis and the solving of systems of non-linear equations), leads to the first known attack on the HAVAL algorithm. Besides that, a new method is developed for the cryptanalysis of the hash mode of PANAMA, a cryptographic module which can be used for both hashing and stream encryption. The second part considers hash functions which are based on a secret key (these are also known as message authentication codes or MAC algorithms). We propose a new design, Two-Track-Mac, based on the two-trail construction that underlies the hash function RIPEMD-160. Our evaluation of this algorithm shows that it offers a large security level against all known strategies of attack. Another advantage is the efficiency, especially in applications where short messages are hashed or where the

key is frequently changed. In those cases Two-Track-MAC performs better than other known constructions such as HMAC and MD<sub>x</sub>-MAC. We submitted our algorithm to the European NESSIE project, which had the goal of proposing a portfolio of secure cryptographic algorithms of the next generation. In February 2003 the NESSIE consortium announced that Two-Track-MAC is selected for the portfolio. Finally, the relation between hash functions and block ciphers is examined, and an attack is demonstrated on the block cipher ICE. This attack is a key-dependent variant on the technique of differential cryptanalysis.

- **G. Rouvroy,**  
**Secure and reconfigurable hardware decoder for digital cinema games,**  
Université Catholique de Louvain, Belgium, June 17, 2004.  
Supervisors: Prof. J.D. Legat and Prof. J.J. Quisquater.
- **R.A. Sitters,**  
**Complexity and approximation in routing and scheduling,**  
TU Eindhoven, May 24, 2004.  
Supervisors: Prof.Dr. J.K. Lenstra, Prof.Dr. J. Sgall.
- **F.-X. Standaert,**  
**Secure and efficient use of reconfigurable hardware devices in symmetric cryptography,**  
Université Catholique de Louvain, Belgium, June 17, 2004.
- **P. Vandecasteele,**  
**On the classification of dense near polygons with lines of size 3,**  
Universiteit Gent, Belgium, December 17, 2004.  
Supervisors: Dr. B. De Bruyn and Prof.Dr. F. De Clerck.  
**Abstract:**  
Near polygons are introduced by E. Shult and A. Yanushka in 1980. We present some new classification results concerning near polygons, where we mainly focus on the so-called slim dense ones, assuming that the existence of quads and that all lines have size 3. All slim dense near hexagons were classified by B. De Bruyn, up to isomorphism there are 11 examples. A similar classification for the slim dense near octagons is proved, there are 24 examples. In order to prove this result the necessity arose to study the possible relation between a point and a geodetically closed sub near hexagon (a hex) of a near polygon. We tackle this problem in a more general context and investigate the possible relations between a point and any geodetically closed sub near polygon. It turns out that each such relation can be described by a valuation, which is a map from the point set of the considered sub near polygon to the set of natural numbers, satisfying a number of nice properties. We studied in particular the valuations of dense near hexagons and classical near polygons (the dual polar spaces). After classifying all possible valuations of the 11 slim dense near hexagons, we determined all slim dense near octagons having a big hex. We finally proved that all slim near octagons need to have a big hex, which leads then to the classification of the 24 slim dense near octagons.
- **André Weimerskirch,**  
**Authentication in ad-hoc and sensor networks,** Ruhr Universität Bochum, Germany, July, 2004.  
Supervisor: Prof.Dr.-Ing. C. Paar.

- **S. De Winter,**  
**Constructions, characterizations and classifications of SPG-reguli,  
 SPG-systems and the related semipartial geometries,**  
 Universiteit Gent, Belgium, December 22, 2004.

Supervisors: Prof.Dr. J.A. Thas and Prof.Dr. F. De Clerck.

**Abstract:**

Two interesting construction methods for (semi)partial geometries are due to Thas. The first one uses so-called SPG-reguli, a particular type of configuration of subspaces of a finite projective space. The second one uses so-called SPG-systems, which are a particular configuration of next to maximal totally singular subspaces of a finite classical polar space. In our dissertation we investigate these configurations as well as the geometries arising from them. After two introductory chapters the next three chapters deal with characterizations and classification of the semipartial geometries that arise as a linear representation, or equivalently, from an SPG-regulus consisting of points. Chapter 3 provides a characterization of the semipartial geometries  $T_2^*(\mathcal{B})$  and  $T_2^*(\square)$  which generalizes a result that was known for the partial geometry  $T_2^*(\mathcal{K})$ . In chapter 4 we obtain the classification of semipartial geometries with a linear representation in the four dimensional affine space  $AG(4, q)$ , the smallest case that was not solved yet. Using results of De Clerck and Delanote, and De Feyter we obtain then the classification of semipartial geometries (that are no partial quadrangles) embedded in  $ag(4, q)$ . In the fifth chapter it is shown that, under a very mild restriction, every SPG regulus with a specific relation between its parameters is the image of the points of a Baer-subgeometry under field reduction. In Chapter 6 sets of subspaces of a projective space satisfying the so-called polar property are studied and their link with SPG-reguli is explained. Several well known objects are encountered here: unitals, ovoids,  $m$ -systems, ... In Chapter 7 a theory of translation semipartial geometries is introduced. It turns out that, with possibly a finite number of exceptions, these geometries provide an alternative description for the semipartial geometries constructed from an SPG-regulus. In this new setting several results, especially about the automorphism group, are obtained. Also, generalized quadrangles admitting a regular abelian group are shown to arise necessarily from a generalized hyperoval. In the next chapter we construct a new SPG-regulus and show that the semipartial geometry arising from it is also new. The results obtained in Chapters 6 and 7 turn out to be very useful in this context. Finally, in the last chapter, SPG-systems are studied. In the singular case a complete classification is obtained, while in the non-singular case we provide a classification of all SPG-systems of index 2.

- **T. Wollinger,**  
**Software and hardware implementation of hyperelliptic curve  
 cryptosystems,** Ruhr Universität Bochum, Germany, May, 2004.  
 Supervisor: Prof.Dr.-Ing. C. Paar.

### 7.3 Ph.D. Committees

- G. Brinkmann  
 – D. Van Dyck, Universiteit Gent, May 2004.
- H.J. Broersma

- Xinming Tang, International Institute for Geo-Information Science and Earth Observation/Universiteit Twente, Enschede, January 9, 2004.
- A. Netchaev, Universiteit Twente, Enschede, September 24, 2004.
- B. De Bruyn
  - P. Vandecasteele, Universiteit Gent, Belgium, December 17, 2004.
- F. De Clerck
  - P. Vandecasteele, Universiteit Gent, December 17, 2004.
  - S. De Winter, Universiteit Gent, December 22, 2004.
- K. Coolsaet
  - P. Audenaert, Universiteit Gent, February 2004.
  - D. Van Dyck, Universiteit Gent, May 2004.
- H. Dobbertin
  - G. Leander, Universität Bochum, Germany, 2004.
- J.-P. Doignon
  - Olivier Anglada, *Quelques polyèdres combinatoires bien décrits*, Université d'Aix-Marseille, 2004.
- V. Fack
  - D. Van Dyck, Universiteit Gent, May 2004.
- C. Hoede
  - Chairman of the committee of Ph.D. defenses of the University of Twente in 5 cases.
- M. Labbé
  - S. Dewez, Université Libre de Bruxelles, Belgium, June 8, 2004.
- D. Leemans
  - Th. Libert, Université Libre de Bruxelles, 2004.
- J.K. Lenstra
  - R. Sitters, TU Eindhoven, May 24, 2004.
- H. Van Maldeghem
  - J. De Beule, UGent, May 20, 2004,
  - G. Deschrijver, UGent, November 9, 2004,
  - P. Vandecasteele, UGent, December 17, 2004,
  - S. De Winter, UGent, December 22, 2004.
- C. Paar
  - J. Guajardo, RUB, Bochum, Germany, July 2004.
  - A. Weimerskirch, RUB, Bochum, Germany, July 2004.

- T. Wollinger, RUB, Bochum, Germany, July, 2004.
- B. Preneel
  - M. Quisquater, KU Leuven, Belgium, May 17, 2004.
  - B. Van Rompay, KU Leuven, Belgium, June 30, 2004.
- J.-J. Quisquater
  - G. Rouvroy, Université Catholique de Louvain, Belgium, June 17, 2004.
- L. Storme
  - H. Van Dierendonck, Universiteit Gent, January 20, 2004,
  - P. Audenaert, Universiteit Gent, April 28, 2004,
  - J. De Beule, Universiteit Gent, May 18, 2004,
  - P. Vandecasteele, Universiteit Gent, December 17, 2004,
  - S. De Winter, Universiteit Gent, December 22, 2004.
- L. Stougie
  - R. Sitters, TU Eindhoven, May 24, 2004.
  - A. van der Kraaij, Universiteit Maastricht, November 12, 2004.
- J.A. Thas
  - J. De Beule, Universiteit Gent, May 20, 2004
  - P. Vandecasteele, Universiteit Gent, December 17, 2004
  - S. De Winter, Universiteit Gent, December 22, 2004.
- K. Thas
  - J. De Beule, Universiteit Gent, May 20, 2004.
- H.C.A. van Tilborg
  - B.M.H. Custers, Universiteit van Tilburg, October 22, 2004.
- J. Vandewalle
  - M. Quisquater, KU Leuven, Belgium, May 17, 2004.
  - B. Van Rompay, KU Leuven, Belgium, June 30, 2004.
- Ph. Vincke
  - S. Dewez, Université Libre de Bruxelles, Belgium, June 8, 2004.
- A.J. Han Vinck
  - S. Mietens, TU Eindhoven, February 2004.
  - H. Hrasnica, Universität Dresden, May 2004.
- A.J. van Zanten
  - W. Groenevelt, TU Delft, June 7, 2004.
  - M. Winands, Universiteit Maastricht, November 1, 2004.

## 7.4 Editorships

- K.I. Aardal
  - Chairman of the publications committee of the Mathematical Programming Society, since 2001.
  - Operations Research Letters, associate editor, since 1998.
  - INFORMS Journal on Computing, associate editor, since 1999.
  - Mathematical Programming B, associate editor, since 2000.
  - Networks, associate editor, since 2003.
  - One of three central moderators for "Optimization Online", [www.optimization-online.org](http://www.optimization-online.org), since 2000.
- A.G. van Asch
  - Euclides, member editorial board.
- H.J. Broersma
  - Contributing editor for International Abstracts in Operations Research.
  - Member of the editorial board of *Discussiones Mathematicae – Graph Theory*.
  - Member of the editorial board of *Graphs and Combinatorics*.
  - Associate editor of *Networks*.
  - Member of the editorial board *AKCE International Journal of Graphs and Combinatorics*.
  - Guest editor of *Electronic Notes in Discrete Mathematics*.
  - Guest editor of *Discrete Applied Mathematics*.
- A.E. Brouwer
  - Editor of *European Journal of Combinatorics*.
  - Editor of *Alg. J. Comb.*
- Ph. Cara
  - Editor of *Innovations in Incidence Geometry*.
- J.-P. Dognon
  - Member of the board of editors of *Mathématiques et Sciences Humaines*, Paris.
  - Member of the board of editors of *Journal of Mathematical Psychology*, Academic Press.
  - Member of the board of editors of *Order*.
  - Member of the board of editors of *Mathematical Social Sciences*.
- A.M.H. Gerards
  - Co-editor of *Mathematical Programming, Series A*, since 2003.
  - Editor of *CWI Tracts*, *CWI Syllabi*, since 1999.
  - Editor of *SIAM Journal on Discrete Mathematics*, since 1999.

- J.L. Hurink
  - Guest editor of Discrete Applied Mathematics.
- M. Laurent
  - Editor of the SIAM Journal on Optimization, since January 2001.
  - Associate editor of Mathematics of Operations Research, since August 2001.
  - Member of the editorial board of the MPS-Siam book series on Optimization, since September 2003.
- A.K. Lenstra
  - Editor of Journal of Cryptology.
- J.K. Lenstra
  - Member editorial board CWI Monographs, CWI Tracts, CWI Syllabi, since 1984.
  - Editor Handbooks in Operations Research and Management Science, North-Holland, since 1998.
  - Member editorial advisory board Kluwer Series in Operations Research/Computer Science Interface, since 1991.
  - Member editorial board Princeton Applied Mathematics Series, Princeton University Press, since 2000.
  - Member advisory board SCIMA Special Series, since 1979.
  - Member advisory board ACM Journal of Experimental Algorithmics, since 1995.
  - Member editorial board Chinese OR Transactions, since 2001.
  - Member advisory board Excerpta Informatica, since 1985.
  - Member advisory board INFORMS Journal on Computing, since 2003.
  - Advisory editor Mathematics of Operations Research, since 1999.
  - Editor-in-chief, Operations Research Letters, since 2002.
- H. Van Maldeghem
  - Editor-in-chief of Advances in Geometry, Bulletin of the Belgian Mathematical Society – Simon Stevin.
  - Managing editor of Innovations in Incidence Geometry.
  - Managing editor of Innovations in Incidence Geometry.
- T. De Medts
  - Assistant managing editor of Innovations in Incidence Geometry.
- G.R. Pellikaan
  - Editor Proceedings of the 25th Symposium on Information Theory in the Benelux, Kerkrade, June 2–4, 2004, Werkgemeenschap voor Informatie- en Communicatietheorie, Eindhoven.
- L.A.M. Schoenmakers

- Editor of deliverable of PROVILAB (WG2), ECRYPT, Network of Excellence in Cryptography.
- A. Schrijver
  - Advisory editor Journal of Combinatorial Optimization, since 1996.
  - Advisory editor North-Holland Mathematical Library, since 1995.
  - Editor Discrete Applied Mathematics, since 1988.
  - Editor Journal of Combinatorial Theory, Series B, since 1993.
  - Editor Journal of Combinatorics, Information and System Sciences, since 1992.
  - Editor SIAM Journal on Discrete Mathematics, since 1988.
  - Editor-in-chief Combinatorica, since 1993.
  - Member editorial board SIAM Monographs on Discrete Mathematics and Applications, since 2000.
- L. Storme
  - Editor Serdica Mathematical Journal (<http://www.math.bas.bg/~serdica>).
  - Managing editor of Innovations in Incidence Geometry.
- J.A. Thas
  - Editor Bulletin of the Belgian Mathematical Society Simon Stevin.
  - Editor Atti Seminario Matematica e Fisico dill 'Universita' di Mod-  
erra.
  - Editor Journal of Algebraic Combinatorics.
  - Editor Annals of Combinatorics.
  - Managing editor Innovations in Incidence Geometry.
- K. Thas
  - Assistant managing editor of Innovations in Incidence Geometry.
- F.M.J. Willems
  - Associate editor European Transactions on Telecommunications (ETT).
- G.J. Woeginger
  - Editor Acta Cybernetica.
  - Associate editor INFORMS Journal on Computing.
  - Associate editor Journal of Scheduling.
  - Associate editor Journal of Discrete Algorithms.
  - Associate editor Networks.
  - Editor SIAM Journal on Optimization.
  - Editor Discrete Mathematics and Theoretical Computer Science.
  - Area editor Operations Research Letters.
  - Editor Discrete Optimization.

## 7.5 Organization of workshops and conferences

- A.G. van Asch
  - Member committee "Vakantiecursus Wiskunde" (CWI).
- Ph. Cara
  - Co-organizer of the Brussels-Ghent seminar on Incidence geometry (6 sessions of 3 talks per year).
- F. De Clerck,
  - Co-organizer (with L. Storme, J.A. Thas and H. Van Maldeghem) of the International Conference on Incidence Geometry, Floreal Club, La Roche-en-Ardenne, Belgium, May 23–29, 2004.
- K. Coolsaet
  - Organizer of the minisymposium "Non-numerical algorithms" at NMC2004 (Dutch Belgian Mathematical Conference), Tilburg, April 16–17, 2004.
- E.R. van Dam
  - Organizer (with W.H. Haemers) of the Dutch-Belgium Mathematical Conference, April 16–17, 2004.
- T.S.H. Driessen
  - Co-organizer of Third Amsterdam-Twente workshop on Cooperative Game Theory and Economics, with second Dutch-Russian Symposium; Tinbergen Institute of Economic Research, Amsterdam, The Netherlands, June 29 – July 1, 2004.
- A.M.H. Gerards
  - Member Programming Committee IPCO X (Integer Programming and Combinatorial Optimization), New York, NY, June 9–11, 2004.
- W.H. Haemers
  - Organizer (with E.R. van Dam) of the Dutch-Belgium Mathematical Conference, April 16–17, 2004.
  - Organizer Operations Research 2004, September 1–3, 2004.
- D. Jibeteau
  - Member organizing committee 8th International Workshop on High Performance Optimization Techniques (HPOPT 2004), CWI, Amsterdam, June 23–25, 2004.
- P. Korteweg
  - Co-organizer (with L. Stougie) of the EIDMA Combinatorial Optimization Reading Group.
- T. Lange
  - Organizing chair, "Elliptic Curve Cryptography - ECC 2004", Bochum, Germany, September 2004.

- Organization of Oberwolfach seminar together with Gerhard Frey, Essen, Germany, 2004.
- Program committee memberships: CHES'04, SCN'04, Indocrypt 2004.
- M. Laurent
  - Member of the organizing committee 8th International Workshop on High Performance Optimization Techniques (HPOPT 2004), CWI, Amsterdam, June 23–25, 2004.
  - Member of the Program Committee of the third EuroComb conference, Berlin, September 5–9, 2005
- D. Leemans
  - Co-organizer of the Universiteit Ghent - Université Libre de Bruxelles, seminar on finite geometries and buildings.
  - Organizer of the seminar "Geometrie, Combinatoire et Theorie des Groupes", Université Libre de Bruxelles. Two meetings in 2004.
- A.K. Lenstra
 

Program committee member of:

  - Asiacrypt 2004.
  - Eurocrypt 2004.
  - Financial Crypto 2004.
  - ICISC 2004.
  - Indocrypt 2004.
  - PKC 2004.
  - SAC 2004.
  - SAC2004.
- J.K. Lenstra
  - Member Program Committee 7th Workshop on Models and Algorithms for Planning and Scheduling Problems, Siena, Italy, June 2005.
- H. Van Maldeghem,
  - Co-organizer (with F. De Clerck, L. Storme and J.A. Thas) of the International Conference on Incidence Geometry, Floreal Club, La Roche-en-Ardenne, Belgium, May 23–29, 2004.
- B. Mühlherr
  - Co-organizer the Oberwolfach-conference 'Buildings and Curvature', May 9-14, 2004.
- C. Paar
  - Organizing chair, "Elliptic Curve Cryptography - ECC 2004", Bochum, Germany, September 2004.
  - Program committee "Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC", Italy, July 2004.
  - Program chair "escar - Embedded Security in Cars", Bochum, Germany, November 2004.

- L.A.M. Schoenmakers
  - Member of program committee of IWAP 2004.
  - Member of program committee of PKC 2005.
  - Member of program committee of Financial Cryptography 2005.
  - Member of program committee of Eurocrypt 2005.
- L. Storme
  - Organizer of the cryptography session for the Dutch Belgian Mathematical Conference, Tilburg University, The Netherlands, April 16–17, 2004.
  - Co-organizer (with F. De Clerck, J.A. Thas and H. Van Maldeghem) of the International Conference on Incidence Geometry at Floreal Club, La Roche-en-Ardenne, Belgium, May 23–29, 2004.
- L. Stougie
  - Member organizing committee Bertinoro Workshop on Combinatorial Optimization (with M. Skutella, Max Planck Institut, Saarbruecken and M. Goemans, MIT, Cambridge, USA), Bertinoro, Italy, May 1–7, 2004.
  - Member organizing committee IFIP-Workshop on Stochastic Integer Programming (with M. van der Vlerk and W. Klein Haneveld, University of Groningen), Groningen, May 24–26, 2004.
  - Member organizing committee EIDMA minicourse Combinatorial Optimization by Éva Tardos, TU Eindhoven, may 10–14, 2004.
- J. Thas
  - Co-organizer (with F. De Clerck, L. Storme and H. Van Maldeghem) of the International Conference on Incidence Geometry, Floreal Club, La Roche-en- Ardenne, Belgium, May 23–29, 2004.
  - Member Advisory Board of "Com 2 MaC Conference or Associations Schemes, Codes and Designs", Pusan National University, Pusan, Korea, July 19–23, 2004.
- A.J. Han Vinck
  - Chairman AEW, Workshop on Concepts in Information Theory, Viareggio, Italy, October 6–8, 2004.
- G.J. Woeginger
  - Member of the program committee of the 3rd Cologne-Twente Workshop on Graphs and Combinatorial Optimization (CTW'2004), Milano, Italy, May 2004.
  - Member of the program committee of the Workshop on On-line Algorithms (OLA'2004), Rungstedgaard, Denmark, July 2004.
  - Member of the program committee of the 31th International Colloquium on Automata, Languages and Programming (ICALP'2004), Turku, Finland, July 2004.
  - Member of the program committee of the 12th European Symposium on Algorithms (ESA'2004), Bergen, Norway, September 2004.

- Member of the program committee of the 2nd Workshop on Algorithmic Methods and Models for Optimization of Railways (AT-MOS'2004), Bergen, Norway, September 2004.
- Member of the program committee of the 1st International Workshop on Parameterized and Exact Computation (IWPEC'2004), Bergen, Norway, September 2004.
- Member of the program committee of the Slovenian Conference on Theoretical Computer Science (IS04-TCS), Ljubljana, Slovenia, October 2004.
- Member of the program committee of the 14th Annual International Symposium on Algorithms and Computation (ISAAC'2004), Hong Kong, China, December 2004.
- Member of the program committee of the 10th International Workshop on Combinatorial Image Analysis (IWCIA'2004), Auckland, New Zealand, December 2004.

## 7.6 Memberships

- K.I. Aardal
  - Member of the program committee of the European Symposium on Algorithms, Bergen, Norway, September 14–17, 2004.
  - Member of the board of directors of the INFORMS Computing Society, 2003-2005.
  - Chairman of the Executive Committee of the Mathematical Programming Society, since 2004.
- Ph. Cara
  - Member of the executive board of the Belgian Mathematical Society.
  - Member of the European Mathematical Society.
- J.-P. Doignon
  - Chairman of the jury of the Belgian Mathematical Olympics (french-speaking part).
  - Chairman of the FNRS Contact Group “Modèles mathématiques en sciences humaines”.
- A.M.H Gerards
  - Board member Landelijk Netwerk Mathematische Besliskunde (since 2001).
  - Member IPCO Steering Committee, Mathematical Programming Society (since 2002).
  - Member of the Science committee of the Thomas Stieltjes Institute for Mathematics (since 2004).
  - Member-at-large of the Council of the Mathematical Programming Society (since 2003).
- A.K. Lenstra
  - Member of the board of the International Association for Cryptologic Research.

- J.K. Lenstra
  - Member Akademie Raad voor de Wiskunde, since 1994.
  - Member Advisory Board Baruch Prize, since 2004.
  - Member Jury VVS-OR 2995 Van Dantzig Prize.
  - Member Scientific Advisory Board Schloss Dagstuhl, since 2004.
- H. Van Maldeghem
  - Member of the board of the Belgian Mathematical Society.
  - Vice-secretary of the National Committee for Mathematics (Belgium).
  - Spokesman of the FWO Research Network Fundamental Methods and Techniques in Mathematics, Belgium.
- L.A.M. Schoenmakers
  - Advisor in cryptography at Philips Research Labs (one day a week).
  - Visiting scientist (CWI, Ronald Cramer's group).
- C. Paar
  - Member steering committee of the CHES conference series.
  - Member IEEE. —item Member ACM.
- L. Stougie
  - Member of the Management Committee of COST-Action 293 GRAAL of the EC.
  - Member of the Steering Committee of the Stieltjes Research Theme Mathematics and Biology.
  - Co-author of the DIAMANT-proposal for NWO Wiskunde-Cluster.
- A. Schrijver
  - Member Algemeen Bestuur Landelijk Netwerk Mathematische Besliskunde (since 1989).
  - Member Advies-Commissie Wiskunde (ACW), Nederlandse organisatie voor Wetenschappelijk Onderzoek (since 2002).
  - Member of the board of EIDMA (since 1993).
  - Member Akademie Raad voor de Wiskunde (since 1995).
  - Member Koninklijke Nederlandse Akademie van Wetenschappen (since 1995).
  - Member Program Board for Mathematics, Lorentz Center Leiden (since 2003).
  - Member Programma Commissie Netwerken, Nederlandse organisatie voor Wetenschappelijk Onderzoek (since 2000).
  - Member Raad van Advies voor de Wiskunde, TU Eindhoven (since 2000).
  - Member Science council Stieltjes Instituut voor Wiskunde (since 1992).
- L. Stougie
  - Member of the steering committee of the Stieltjes Research Theme Mathematics and Biology.

- J.A. Thas
  - Member of the Scientific Board of EIDMA
  - Member of the Royal Flemish Academy of Belgium for Science and the Arts.
  - Secretary of the National Committee for Mathematics.
- TNO Telecom is a member of NEN norm commission 381027. This commission determines the National standpoint (i.e. vote) in ISO JTC1 SC27, IT Security.
- T. Veugen
  - Member of the expert group Security and Control of the Electronic Commerce Platform of the Netherlands (ECP.NL).
  - Member of the user committee of the STW project DIWAMETRIC.
  - Member of the user committee of the Gencom project BASIC.
  - Member of the IFIP working group 11.4: "Network and Distributed Systems Security".
- A.J. Han Vinck
  - IEEE member transnational committee.
  - IEEE member Section/Chapter support committee.
  - IEEE Information theory Society past president.
  - Elected Member Editorial Board IEICE, Japan.
  - Member of the Board of EIDMA.
  - Member of the Board of the Working Community on Information Theory in the Benelux.
- B. de Weger
  - Program committee member of the WIC Symposium, Kerkrade, June 2-4, 2004.
- Dr. F.M.J. Willems
  - Fellow IEEE.
  - Advisor on Information Theory for Philips Research Laboratories, Eindhoven.
- G.J. Woeginger
  - Member of the steering committee of the European Symposium on Algorithms (ESA).
  - Member of the council of the European Association for Theoretical Computer Science (EATCS).
  - Member of the Program Board for Computer Science of the Lorentz Center (Leiden).
  - Member of the steering committee of the Workshop on Models and Algorithms for Planning and Scheduling Problems (MAPSP).
  - Member of the advisory committee of the Multidisciplinary International Conference on Scheduling: Theory and Applications (MISTA).