

## Part C: New cluster plans

### 1 Research plan

#### 1.1 The different research themes

The formation of the new DIAMANT board, in which a younger generation of scientists has taken the lead, also reflects a number of changes in the research accents found inside the cluster. These changes are discussed in some more detail in section C.5. Below we identify five main research themes. Note that, due to the changes to be discussed below, these themes differ slightly from the five research areas that were identified in Part B.

#### A. Number theory and arithmetic geometry

The second half of the 20<sup>th</sup> century has seen spectacular advances in number theory and algebraic geometry, and many of these focus in one way or another on the structure of the set of solutions to systems of polynomial equations, or connections between number theory and representation theory of matrix groups (Langlands program). The 1995 proof by Wiles of Fermat's Last Theorem is a concrete and widely known illustration of the power of the combination of techniques from number theory and algebraic geometry. Advances in this area are often viewed as being of an abstract and rather technical nature, but they will undoubtedly gain clarity and added importance from the application to concrete mathematical problems that we have in mind. In order to obtain such concrete applications, much of the heavy machinery needs to be made *explicit* in order to be of use in the more algorithmic settings that are central to this theme, and to DIAMANT as a whole.

#### Research directions:

The efficient computation of coefficients of modular forms is a challenging instance of what can be seen as part of what may be broadly referred to as an *explicit Langlands program*. It is directly related to the point counting algorithms over finite fields for elliptic curves and more general algebraic varieties, and to explicit computations of the Galois representations arising from the natural action of the absolute Galois group of the rational number field on ubiquitous arithmetic algebraic objects such as abelian varieties. Algorithms in this area are diverse, and come in various degrees of concreteness: in some cases there are only experimental algorithms, in others we have working algorithms but no estimates of their asymptotic run time, and in some well-studied cases (arithmetic of elliptic curves) we are at the point of optimizing proven run times by making intelligent coordinate choices.

More classical algorithms will also remain a topic of research in this theme. They include factoring algorithms based on the number field sieve and the elliptic curve method, as their practical performance has direct implications for "secure" cryptographic primitives. Also, lattice reduction algorithms as LLL can be used in a wider variety of applications when suitably generalized to the context of *layered lattices*.

In the area of Diophantine equations, we are now starting to extend classification results of the kind that exist for curves (in terms of the genus) to the case of algebraic surfaces, although much is still conjectural at this point.

The topic of arithmetic equivalence, or equality of zeta functions, which arose in the context of number fields, has regained interest in the context of function fields with characteristic- $p$  zeta functions lifted to characteristic zero, and in similar settings in differential geometry. They also arise as partition functions for certain physical systems.

Several topics that will be studied by DIAMANT researchers are on the borderline between this theme and others. On the borderline with the logic theme there are the analogues of division polynomials and divisibility sequences in higher genus, and their relation to first-order definability of the integers in the rational numbers and algorithms for Diophantine equations. Close to combinatorics we find the ergodic properties of number expansions and the use of finite automata in continued fractions.

#### B. Cryptology

Cryptology studies the extent to which problems pertaining to security in the presence of malicious adversaries can be solved by means of data processing, and, where it applies, how this can be done efficiently. For example, encryption schemes and digital signatures are used to construct private and authentic communication channels ("unilateral security," security against malicious outsiders). These are instrumental to secure Internet transactions and payments, mobile telephony and much more. Another example is secure computation, which in principle enables an arbitrary computation to be distributed among the processors in a network so that computations remain secret and are performed correctly, even if a certain quorum of the network is under full control by an adversary ("multi-lateral security,"

security among mutually distrusting parties or parties with conflicting interests). Besides being a versatile theoretical primitive, potential real-life applications are myriad and include secure cooperation in the absence of trust, auctions, privacy-protecting data-mining and benchmarking. Notable examples that fit neither security category include secure positioning and searching encrypted data.

The research in cryptology is driven partly by questions such as: How reliable are the cryptographic methods in use today, really? Can they be made more secure and/or more efficient? Which are possible (minimal) assumptions under which security can be provided? Post-quantum cryptography: what to do if and when life-size quantum computers come into existence, and, hence, today's standards for secure communication are rendered insecure? Can large-scale secure computations be made practical? Advances in modern cryptology increasingly rely on deeper understanding of interplays with algebra, number theory, geometry, combinatorics, probability theory, complexity theory, formal methods, quantum physics and information theory.

#### Research directions:

RSA is still the de facto industry standard for public key cryptography. The Number Field Sieve Project (NFS) has contributed substantially to the understanding of the security of RSA, and, through its important cryptanalytical success the last 20 years, it has de facto determined the key lengths for various industrial applications. These key-lengths turned out to be necessarily much higher than what was expected *before* the NFS Project was started. Elliptic Curve Cryptography (ECC) is now in the process of becoming an important industry standard, side-by-side with RSA, after resisting more than two decades of cryptanalytic scrutiny. Yet, theoretical and practical research into its security must be continued, and limits must be pushed as far as possible. Also, several variations on the original ECC are under consideration, typically for enhanced functionality, such as pairing-based cryptography. Further study into the security and the efficiency of such methods is also called for. Another important question is whether ECC can be made more efficient so that it can run on devices with low resources.

Essentially all the cryptographic schemes that are currently used in industry can in theory be broken by means of a quantum computer. This is due to the fact that their security relies on the hardness of such problems as factoring large integers or computing discrete logarithms, which are easy on a quantum computer. Although building a scalable quantum computer is currently out of scope, this may very well pose a serious threat in the future. The goal of post-quantum cryptography is to develop the theory and practice of cryptographic schemes that resist quantum attacks.

A promising approach is to base security on the hardness of computational problems that arise in the geometry of numbers. It is an important goal to exhibit new and efficient cryptographic schemes for various tasks that can be proven secure based on such computation problems from the geometry of numbers. But also: to what extent can cryptography based on the geometry of numbers be cryptanalyzed by (quantum) computational number theory? How should the key-lengths be chosen? Also, is cryptography based on coding theory a possible alternative?

Besides cryptanalytical methods, quantum information processing and quantum cryptography bring functionalities that cannot be achieved by means of "classical" (i.e., non-quantum) cryptography. Recently, quantum cryptography brought forth a solution to the "secure positioning problem." This is of great potential practical interest, and it has very promising theoretical connections to non-locality and combinatorial optimization, in particular linear and semidefinite programming. In general, what are the limits of quantum cryptography, how efficient can it be?

There are several initiatives underway where economic fairness is achieved through secure multi-party computation. Game-theorists and economists are currently discovering the power of secure multi-party computation. Can secure combinatorial optimization be made practical? Also, in recent years, deep theoretical connections between secure multi-party computation and algebraic geometry have been discovered, the limits of which have yet to be understood.

Several hash-functions have been cryptanalyzed successfully in recent years. A reliable approach to the design of such schemes appears to be lacking. How does one design secure hash-functions?

Side-channel attacks bypass cryptography and break security by exploiting information-leakage from the devices that operate cryptography (measurement, timing, etc). An example is the "OV-chipcard disaster." Previous solutions to side-channel attacks were very ad-hoc and typically tailored to known attacks. There is currently great effort in developing systematic ways to defeat side-channel attacks, which are based on well defined theoretical models for the information that may (and may not) leak as a result of a side-channel attack. The goal is to exhibit cryptographic schemes that are secure with respect to realistic models for the information leakage that should not only cover currently known side-channel attacks—like (differential) power analysis, cold-boot attacks etc.—but also potential future side-channel attacks.

The complexity of security systems steadily increases, and hence the need arises for a modular approach to security analysis. Can one devise a general composition theory for security? Can security analysis/proofs be automatized?

### *C. Optimization*

The objective is to develop structural results and efficient algorithmic methods for solving hard optimization problems. To achieve the goals we combine tools from several branches of mathematics: Invariant theory is used to exploit problem structure and symmetry in order to develop more compact computational models; commutative algebra and real algebraic geometry are used to attack optimization problems over polynomials; theory of lattices is used to provide results for integer programs; robust optimization is an approach to decision making in environments with significant data uncertainty; polyhedral combinatorics combined with linear and semidefinite programming are basic techniques used to design tight approximations for combinatorial optimization problems; techniques from optimization and algorithms are used to obtain new insights into the characteristics of games and mechanism design; smoothed analysis is used as a tool to derive more realistic performance estimations of algorithms; probabilistic techniques are used to analyze combinatorial and polyhedral structures whose average case behavior under various probabilistic models will be studied. We aim at both developing new techniques for optimization, as well as broadening the scope of optimization.

#### Research directions:

##### *I) New techniques for optimization*

SDP and beyond: A common feature of integer and non-convex quadratic optimization problems is that the computational effort explodes with the dimension. Semidefinite programming (SDP) has been developed as a possible way to cope with these difficulties. Here, one transforms to a higher-dimensional matrix space to obtain a problem that is efficiently solvable. SDP has a large expressive power and is versatile, but in transforming a problem, some information is usually lost, so that the transformed problem is just an approximation of the original problem. An alternative is optimizing over the cone of copositive matrices. In many types of combinatorial and quadratic problems, the copositive formulation is indeed an exact reformulation rather than a relaxation. The benefit is that one gets linear formulations with a single convex conic constraint that captures all the difficulty of the combinatorial or quadratic problem. This approach opens new ways of dealing with quadratic and combinatorial problems, allowing new insights and better approximations.

Fourier analysis has been widely used in various areas. The principle is simple: a mathematical function is written as a sum of well-chosen basis functions. The resulting Fourier coefficients describe the correlation between the original function and the basis functions, encapsulating properties of the original function. Recently this has gained prominence in the theory of computing (incl. quantum), as well as in combinatorial optimization. It serves as a tool for combinatorial optimization problems such as the kissing number problem, the problem of coloring the Euclidean space and problems in coding theory. Fourier analysis helps identifying symmetries, thereby reducing the number of variables and allowing for a simpler and more compact SDP-formulation.

Attacking symmetries: The feasible regions of many optimization problems exhibit a high degree of symmetry. Standard algorithms do not take advantage of this, and, even worse, many methods are known to work notoriously bad on symmetric problems. Recently, approaches for a variety of specific problems have been developed that exploit symmetries, but there are strong indications that significant algorithmic progress is still possible. To increase the performance of such computational techniques we will develop algorithms and tools that combine optimization methods and computational group theory.

Lattice analysis: For some integer optimization problems, the natural linear relaxation provides very little information on the problem structure. Nor is symmetry the main issue. Such problems can be extremely hard to solve using standard enumerative algorithms, even in low dimension. An alternative is to obtain structural information from the underlying lattice. We intend to use this information algorithmically, and to translate this information into improved linear relaxations.

##### *II) Broadening the scope of optimization*

The classical paradigm for algorithmic research in optimization is the worst case paradigm. This is often too pessimistic, or too narrow by scope.

Robust optimization is an approach to decision making in environments with significant data uncertainty. The objective is to find a feasible solution that performs well under all possible cost/profit realizations. To hedge against parameter variations, one typically uses min/max criteria, for example the min/max

regret. Robust optimization problems often fall beyond the complexity class NP. We want to study the complexity and algorithmic tractability of concrete optimization problems e.g. from scheduling, graphs, and algorithmic game theory.

Smoothed analysis takes into account that typical instances are neither worst-case nor completely random. It measures performance of algorithms on instances subject to a small amount of random noise. This models, for example, measurement or rounding errors and often leads to a more realistic evaluation of the performance of algorithms.

Mechanism design: In settings where problem data are distributed among several agents, optimization techniques have to take into account a new set of constraints, the incentive constraints. They reflect the fact that agents must be incentivized to be truthful. Mechanism design extends the design of optimal algorithms to this more general setting, and gives rise to new insights into the complexity of optimization problems, given a certain paradigm of decentralization.

#### *D. Logic and proof checking*

Mathematical logic was developed in the first half of the twentieth century with the goal of settling questions in the foundations of mathematics. This most pure and foundational of origins has quickly been eclipsed by the pertinence of mathematical logic in modern applications, in particular to fields such as computer and information science. In computer science, the role of logic has been compared to that of analysis for physics. Such areas of computer science as verification, models of computation, and complexity theory are intimately related to logic and provide exciting frontiers of application for pure mathematics. On the other hand, the use of powerful computers also has an impact back in mathematics itself. This may be seen in the area of computer algebra but also in logic where sophisticated logical modeling and powerful computers collaborate to make proof checking and proof assistants possible.

#### Research directions:

Formalization of algebra and analysis in Coq: Mathematics plays an increasingly crucial role in the design of sophisticated systems that are used daily in such areas as geometrical modeling, robotics, and cryptography. Thus issues of correctness and reliability are important. The goal of this project is to make formal proof verification available to new domains. Specifically, the Nijmegen group will extend and refine their existing repository of exact real analysis in order to develop a certified ODE solver in Coq. The further aim is then to merge this with the MathComponents work of Gonthier's group at INRIA and the work on certifying algorithms from computer algebra at Chalmers and La Rioja. This work will be done in the framework of the EU FET STREP project ForMath.

Correctness case studies in computer science—hybrid systems: Hybrid systems are systems that exhibit a combination of discrete and continuous behavior. Important examples include automated transportation systems, process control systems, and systems of embedded devices. Modeling and ascertaining the correctness of such systems is a great challenge as it requires the seamless integration of continuous and discrete behavior. This project will consist of a number of correctness case studies making use of the library of formal mathematics.

MathWiki: The aim of this NWO project is to provide access to proof assistants for a wider community by building a web-based collaborative authoring environment for formal mathematics. This requires further developing Wiki and semantic web technologies in the context of proof assistant repositories including techniques and tools for integrating proof assistants, for interfacing with them, and for documenting formal developments.

Models of computation: Study of the lambda calculus is an ongoing fundamental research theme of the group that plays an important role as the underlying formalism in the applied projects above. In an NWO funded project, algebraic and categorical tools for studying the denotational semantics of the differential lambda calculus will be developed. This calculus is a recent paradigmatic functional programming language enriched with a syntactic derivative operator permitting control of the amount of resources used by a program. The main goals of the project are to formalize abstract notions of models of the calculus, to study concrete examples of these, and to provide general set-theoretical constructions to build classes of models.

Topological duality for ordered algebraic structures: Algebra and topology embody the two fundamental strands of mathematical thinking and often interact in fruitful ways. Dualities between classes of algebras and classes of spaces play a significant role both in logic, where they correspond to the syntactic and semantic approaches, respectively, and in computer science, where they correspond to specification languages and dynamic transition models, respectively. Current projects include a major project on formal languages in automata theory and beyond with CNRS researchers at LIAFA in Paris, an NWO

funded project on continuous and discrete dualities in mathematics and computer science, and a project on duality theory and categorical models of predicate logic.

Logic and probability: While logic is concerned with reasoning, probability concerns formalizations of such notions as randomness, probability, and expectation. The latter is closely related to modeling of inductive inference and learning and thus to some kind of probability logics. Randomness, in the form of algorithmic randomness leads to another connection between logic and probability theory belonging to the area of computability theory that we will explore. It may lead to collaboration with the STAR cluster.

Set theoretic topology: Here our current project concerns a comparative study of the Cech-Stone compactifications of the natural numbers and the positive real line. A topological characterization of the remainder of the Cech-Stone compactification of the positive real line is sought. In this direction, a specific question is whether every perfectly normal continuum is a continuous image of this space.

Interactive mathematical documents: The recent developments in ICT offer new and exciting ways of interacting with and exploration of documents stored on a computer. Within this area of research we develop software to interact with mathematical documents.

### *E. Algebra and combinatorics*

Algebra is the mathematical study of *structures*, collections of objects with operations. These objects may be numbers, matrices, or polynomials, equipped with the operations of addition and multiplication, but they may also be more abstract, such as symmetries of a Platonic solid or points on elliptic curves. But even when the objects of study are of a more abstract nature, it is often possible to *represent* them by more down-to-earth objects such as matrices. To do so is a mathematical challenge, which has gained substantial practical importance during the 20<sup>th</sup> century, as it allows us to manipulate abstract objects on a computer.

Combinatorics is a somewhat ill-defined mathematical term, which we take to comprise all mathematics having to do with *counting* objects in a collection, such as the symmetries of a network or the winning strategies in a game. While many problems in combinatorics are easy to state, their resolution often involves the development of advanced algebraic techniques. On the other hand, deep algebraic results can sometimes be proved by a sophisticated combinatorial analysis of an underlying discrete problem.

Ubiquitous in our research are the notions of *group*, which captures the symmetries of some structure, and *Lie algebra*, a linear approximation to a (continuous) group that is extremely useful in theory as well as in computations. In the 20<sup>th</sup> century, both types of structures have to some extent been classified. The classification of all *finite simple groups* states that such a group is either cyclic, alternating, of Lie type, or one of 26 sporadic examples. The classification of *finite-dimensional modular simple Lie algebras* says that such a Lie algebra in characteristic at least 5 is either classical, of Cartan type, or Melikian. The *groups of Lie type* and the *classical Lie algebras* are strongly related, and form the central parts in both classification results.

#### Research directions:

Finite geometry: This is geometry over finite fields, featuring groups of Lie type over finite fields. Emphasis will be laid on the study of extremal configurations of subspaces with certain intersection properties, where we will profit from recent advances in *geometry over the field with one element* to relate such configurations to the combinatorics of extremal set theory. Put differently, we will develop a *q-analogue* of classical extremal set theory, and attempt to relate the two by letting *q* tend to 1.

Network parameters: Physicists have introduced so-called *edge coloring models* and *vertex coloring models*, which attach quantities to networks that depend only on the isomorphism type of the network. The quest for characterizations of these models naturally leads to questions in invariant theory of algebraic groups. While such characterizations have been obtained for some of these models, among others by DIAMANT-member Schrijver and collaborators, other models turn out to be much harder. We aim to find satisfactory characterizations, not only for the existing commutative models, but also for non-commutative models that yield invariants of graphs-with-extra-structure such as graphs with a cyclic orientation of the edges at every vertex and for infinite-dimensional analogues where the color space is a *Banach space* rather than a finite-dimensional space. This topic is also of interest to theoretical physicists.

Algebraic statistics: Algebraic statistics studies families of algebraic varieties, each of which describes a statistical model on some ground set. One of many challenging tasks consists in finding equations for these algebraic varieties. The action of their natural symmetry groups will be used, along with techniques from computer algebra and representation theory of those symmetry groups, to face this task. There will be special focus on the behavior of these models as the data sets become very large or even infinite.

Another strand of research in this area concerns real-algebraic questions, where not only equations, but also inequalities between real-valued polynomials, convexity issues, and positive definiteness play key roles.

Groups of Lie type, Lie algebras and their geometries: Within the theory of *finite simple groups* the interaction of groups and geometries has been very fruitful. The geometric method in finite group theory has been one of the key ingredients in the theory of finite simple groups. This successful interaction serves as a model for the relations between Lie algebras and geometries that we will explore. Our research will focus on: extending the geometric study of (finite) groups, with applications in the areas of linear groups and permutation groups; investigation of modular Lie algebras by geometric methods, and exploitation of the classification of finite simple groups in the study of various combinatorial structures with symmetry or satisfying regularity conditions.

Algorithms in algebra: A central and unifying effort within DIAMANT consists in making abstract theory *effective* in the form of mathematical algorithms and their implementations. We will develop new algorithms for computations in structures such as Lie algebras, associative algebras (in particular, Brauer-type algebras), and algebraic groups. There will be close collaboration with other areas within DIAMANT, where these algorithms will find important applications—see, for instance, the paragraph on ‘attacking symmetries’ in the Optimization section.

Discrete tomography: This is a research area concerned with the reconstruction of three-dimensional objects from two-dimensional projections. Discrete tomography has a wide variety of applications, ranging from medical imaging to diamond shaping. The group will focus on the design of new algorithms for tomographic reconstruction at all scales.

## 1.2 Coherence

Although we have subdivided the DIAMANT research plans in five themes to facilitate an overview of the cluster research, it goes without saying that any subdivision of mathematical research along thematic lines is partially artificial, and will somewhat arbitrarily designate certain researchers as belonging to one side of a border. In fact, this phenomenon already occurs between the 4 clusters that form the subject of this report. For instance, the algebraic geometers in the Netherlands, who have a record of national cooperation spanning several decades, have now become divided between DIAMANT and GQT. It is therefore no coincidence that GQT board member Cornelissen occurs as a member of DIAMANT as well, and that mathematicians from one cluster regularly take part in activities organized by other clusters. After all, the clusters are not meant to form an ‘impediment’ to collaboration in the Netherlands.

The DIAMANT cluster is built around the algorithmic approach in algebra, discrete mathematics, logic, optimization and number theory, and some of the many ties between the 5 themes it comprises have already been mentioned above.

The most artificial borderline in DIAMANT probably lies between the number theory and crypto themes, and several crypto members might also be called number theorists, and conversely. Given the fact that current cryptographic protocols involve advanced arithmetical concepts, this will not come as a surprise.

In a similar way, the algebra and combinatorics theme intersects the other themes in various ways. The geometry over finite fields can be seen as part of the broader structure of algebraic geometry as practiced by the arithmetic algebraic geometers in the number theory theme, and the study of network parameters is within the field of expertise of many researchers in the optimization theme. Algebraic statistics naturally leads into the topics of the optimization theme.

By its very nature, computer algebra is on the interface of mathematics and computer science as it occurs in DIAMANT. Its DIAMANT practitioners mostly work in number theory, but the link with proof checking and with the investigation of Lie groups and algebras makes it a very central DIAMANT topic.

## 2 Quality of the research team

The DIAMANT cluster was founded by 4 prominent Dutch scholars, who formed the first DIAMANT board. They will still play an important role in the research of the cluster in the coming years, but a new board consisting of five younger mathematicians has now taken over the organization of the cluster. The cv's of all current and former board members follows below.

Clearly, the quality of the research team is not restricted to board members only. DIAMANT now incorporates 28 full professors, 7 associate professors and about 38 assistant professors with appointments at 10 different Dutch universities, including the research center CWI.

*Henk Barendregt* studied mathematics at Utrecht, where he obtained his PhD degree in 1971. He remained at Utrecht until 1986, working first in philosophy and then in mathematics. He was appointed full professor at Nijmegen in 1986, where he presently occupies the Chair of Foundations of Mathematics and Computer Science. He was visiting professor at the ETH Zürich, Kyoto, Wollongong (Australia), and the École Normale Supérieure in Paris. From 1999 until 2005 he was an adjunct professor at Carnegie Mellon (Pittsburgh, USA). In 1992, 1996, and 1997 he was elected to the Academia Europaea, the Koninklijke Hollandse Maatschappij der Wetenschappen, and the Koninklijke Nederlandse Akademie van Wetenschappen. In 1998, his home university awarded him a seven year personal grant, and in 2002 he received the NWO Spinoza award. Barendregt is known for his work in lambda calculus and type theory. His monograph on untyped lambda calculus has been translated into Russian and Chinese.

*Arjeh Cohen* studied mathematics and theoretical computer science at Utrecht, where he obtained his PhD degree in 1975. He worked at the Openbaar Lichaam Rijnmond (Rotterdam), the Technische Universiteit Twente (Enschede), CWI (Amsterdam), and at the Universiteit Utrecht, where he became a full professor in 1990. Since 1992, he has been a full professor of Discrete Mathematics at the Technische Universiteit Eindhoven. He has been the scientific director of RIACA, chairman of the board of the research school EIDMA, and president of the OpenMath Society, and is presently Dean of the Department of Mathematics and Computer Science in Eindhoven. He occupied visiting positions in Ann Arbor, Ber Sheva, Jerusalem, Kobe, Naples, Pasadena, Rome, Santa Cruz, and Sydney. Cohen's main scientific contributions are in groups and geometries of Lie type, and in algorithms for algebras and their implementations. He is also known for his work on interactive mathematical documents. Eighteen students have received a PhD under his supervision. Currently, he is on the editorial board of three research journals and the ACM book series of Springer-Verlag.

*Hendrik Lenstra* obtained his PhD degree at the Universiteit van Amsterdam in 1977, was a full professor in Amsterdam from 1978 until 1986, at the University of California, Berkeley, from 1987 until 2003, and at the Universiteit Leiden since 1998. Lenstra is best known for introducing advanced techniques in the area of number-theoretic algorithms. In 1985 he was awarded the Fulkerson prize by the American Mathematical Society and the Mathematical Programming Society, and in 1998 he was the recipient of an NWO Spinoza award. Since 1984 he has been a member of the Koninklijke Nederlandse Akademie van Wetenschappen, and since 1996 a fellow of the American Academy of Arts and Sciences. In 1990/1991 he held a Distinguished Visiting Professorship in the Institute for Advanced Study (Princeton). He received an honorary doctorate from Besançon in 1995, and since 2007 he has been Akademietoelichtaar. Thirty-five students have completed their PhD theses under his supervision. He is on the editorial board of six research journals and one book series, the *Ergebnisse der Mathematik und ihrer Grenzgebiete*.

*Alexander Schrijver* did his PhD research at the Mathematisch Centrum and obtained his degree from the Vrije Universiteit in Amsterdam in 1977. He specializes in discrete mathematics and optimization. From 1983 until 1989 he was a full professor at Tilburg, after which he joined the Centrum voor Wiskunde en Informatica as a researcher, with a part-time professorship at the Universiteit van Amsterdam. He held visiting positions at Oxford, Szeged, Bonn, Bell Communications Research, Rutgers University, Yale University, and Microsoft Research. In 1982 and 2003 he was awarded Fulkerson prizes by the American Mathematical Society and the Mathematical Programming Society, in 1987 a Lanchester prize by the Operations Research Society of America, and in 2003 a Dantzig prize by the Mathematical Programming Society and the Society for Industrial and Applied Mathematics. Since 1995 he has been a member of the Koninklijke Nederlandse Akademie van Wetenschappen, and in 2002 he received an honorary doctorate from the University of Waterloo in Canada. He is on the editorial board of eight research journals and two book series.

*Karen Aardal* received her PhD in applied mathematics from Université Catholique de Louvain in 1992. She has held faculty positions at the University of Essex (UK), Erasmus University, Tilburg University, Utrecht University, Georgia Tech (USA), CWI, and TU Eindhoven. Since 2008 she is full professor at Delft University of Technology where she heads the Optimization and Systems Theory group. She is an area editor of *INFORMS Journal on Computing*, and an associate editor of *Mathematical Programming B* and *Networks*. She has been the chair of the Executive Committee and the Publication Committee of the Mathematical Programming Society (MPS), a member-at-large of the MPS Council, and a Director of *INFORMS Computing Society*. She was a member of the 2006 QANU assessment panel for Mathematics programs at Dutch universities. Her main research interests are in integer optimization, in particular algebraic methods.

*Tanja Lange* received her PhD in mathematics from the University of Essen in 2002. After three years at Ruhr-University Bochum she joined Technical University of Denmark as Associate Professor and then in

2006 joined Technische Universiteit Eindhoven as Full Professor. Prof. Lange has published more than 50 research papers bridging the gaps between algebraic geometry, theoretical cryptography, and real-world information protection. She is an expert on curve-based cryptography and post-quantum cryptography. She is on the editorial board for 2 journals and serves on 3 steering committees. She has organized around 20 conferences and workshops, has served on more than 40 program committees. She co-leads the Virtual Applications and Implementations Research (VAMPIRE) lab in the European Network of Excellence in Cryptography, and leads the NaCl working group in the EU FP7 project Computer-Aided Cryptographic Engineering.

*Mai Gehrke* received her PhD in mathematics, with specialization in algebra and logic, from the University of Houston in 1987. After several positions as a postdoctoral researcher, she joined the mathematics faculty at New Mexico State University. Over 15 years, she established a group in logic and helped found a complex systems group at the Physical Science Laboratory there. Since 2007 she holds the Chair of Algebra at Radboud University. In addition, Gehrke has spent extended visiting professorships and sabbaticals at the University of Copenhagen, Paris 7, and Oxford University. Her work, counting some 50 publications, focuses on topological methods in the study of ordered algebraic structures, especially as pertinent in theoretical computer science. Gehrke has sat on various national grant committees, program and steering committees, and is an editor of the Houston Journal of Mathematics. She is regularly a plenary speaker at international conferences spanning in subject from algebra through logic to theoretical computer science.

*Ronald Cramer* is head (and founder) of the Cryptology research group at the Centrum Wiskunde en Informatica (CWI) in Amsterdam and holds the Chair in Cryptology within the Algebra & Number Theory group in Leiden. Cramer held research positions at ETH Zürich and at Aarhus University from 1997–2004. He holds a PhD in Cryptology from the University of Amsterdam (1997). In 1998 he received the KNAW Christiaan Huygens Award and in 2006 he won an NWO VICI grant. In 2005 he was elected to De Jonge Akademie (KNAW). From 2004–2007 he was a Director of the International Association for Cryptologic Research (IACR). Cramer is on the editorial board of several journals, including Journal of Cryptology, and served as Program Chair of EUROCRYPT 2005 and of PKC 2008. Cramer's research interests include all aspects of public key cryptography, cryptographic protocol theory and secure computation. In recent years, the focal point of his research is mainly mathematical cryptology.

*Peter Stevenhagen* received his PhD in number theory from the University of California in 1988. He held an appointment as CNRS-researcher in Besançon before founding a number theory group at the University of Amsterdam. In 1993, he started with De Smit the biweekly Intercity Number Theory Seminar that has become the national platform for number theory research in the Netherlands. In 2000, he moved to Leiden, where he is currently department chair. He has organized numerous conferences, and is a frequent speaker worldwide. Besides his research papers on algebraic and algorithmic number theory, his bibliography counts various papers of popularizing and historical nature. With Buhler (CCR San Diego), he authored and edited an authoritative text on algorithmic number theory.