Centrum voor Wiskunde en Informatica

Annual Report 2005

Contents

Centrum voor Wiskunde en Informatica

Visiting Address	Kruislaan 413
	1098 SJ Amsterdam
	The Netherlands
Postal Address	P.O. Box 94079
	1090 GB Amsterdam
	The Netherlands
Telephone	+31 20 592 9333
Fax	+31 20 592 4199
Website	www.cwi.nl

Centrum voor Wiskunde en Informatica (CWI) is the national research institute for mathematics and computer science. It is supported by the Netherlands Organisation for Scientific Research (NWO).
CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics. The institute is a member of the World Wide Web Consortium (W3C) and it manages the W3C Office in the Benelux. CWI is located at Science Park Amsterdam.

CONTENTS

Introduction 5

Overview 6
1. To conduct advanced research of societal and scientific relevance 8
2. To act as a 'breeding ground' for academic staff 15
3. To train young researchers 17
4. To transfer knowledge to society 21
5. To play a leading role in the Dutch and European mathematics and computer science scene 27
6. To increase public interest in mathematics and computer science 30

Research Highlights 34
Mathematics discovers unexpected change in plankton populations 35
Coordination of emergency communication in safe hands 39
MonetDB/XQuery: Searching XML databases in record time 43
Safety measures for future cyber security 47

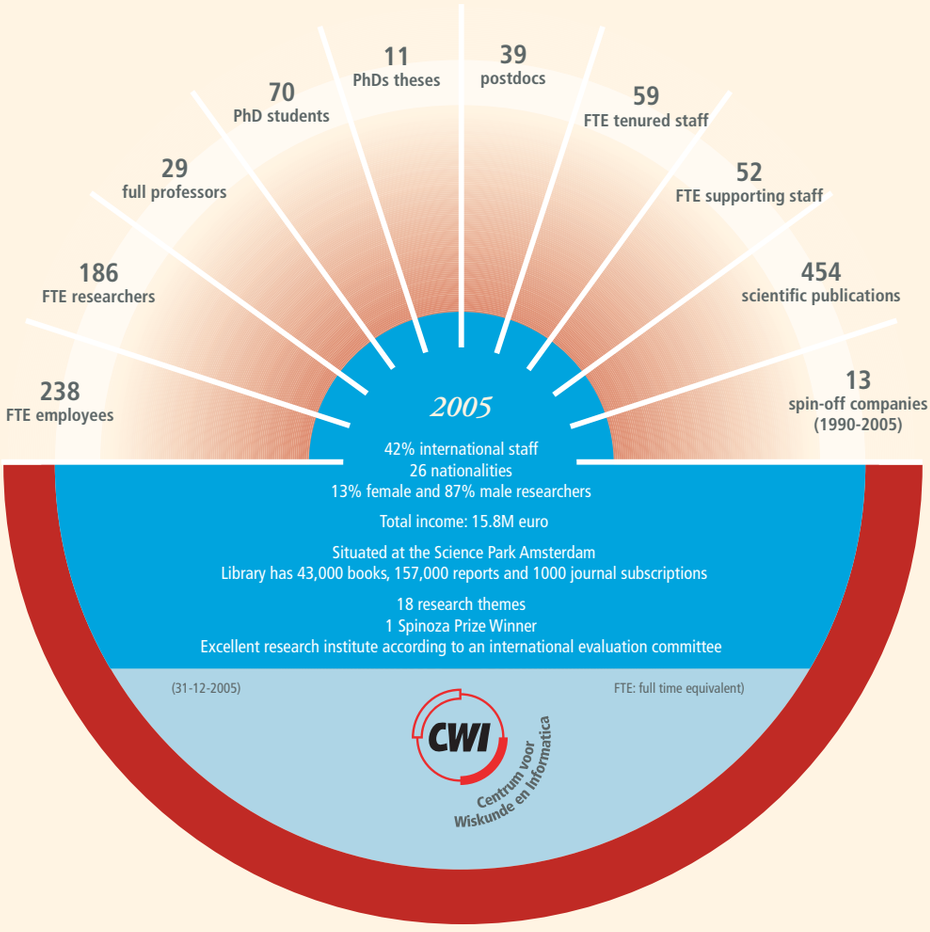
Appendices 50
Organization 51
Facts and figures 52
CWI clusters and themes 55
International and national programmes 62

The CWI annual report series consists of:

- Annual Report (English), a full colour document giving a general overview of CWI's activities
- Overview Research Activities (English), a comprehensive enumeration of CWI's research
- Jaarverslag (Dutch), a supplement containing the social and financial report and the works council report

Copies can be ordered at the Communications, Library and Information services department (CBI): cbi@cwi.nl

Introduction



CWI celebrates its sixtieth anniversary this year, and looks back to 2005 with considerable pride. High points were the rating 'excellent' from an external evaluation, the Spinoza Prize for Lex Schrijver, two royal decorations, the Van Dantzig Prize, the ITEA Achievement Award, two Veni grants, three more full professors, eleven PhDs, and NWO giving us the green light for the construction of a new wing and renovation of the current building.

Every six years, CWI is subjected to an evaluation by NWO, the Netherlands Organisation for Scientific Research. The international committee judged us as 'excellent'. In their eyes CWI is a powerful and vibrant institute. And, of course, we are very proud of this. The committee also indicated some points for improvement. They advise CWI to establish a scientific council, to formulate a strategy for the life sciences, and to reduce the autonomy of the research themes to create more flexibility. On the road to greater efficiency, CWI already realigned its service departments.

To further its position, CWI actively participates in various national and international initiatives. It helped formulate key research questions during the drafting of the national research agenda in ICT for 2005-2010. Apart from stimulating research, this agenda aims to create clarity in the structure of ICT research and to position Dutch research within Europe.

Another initiative to improve and stimulate high-quality research and its interaction with society was the formation of national mathematical clusters. Three clusters were selected in 2005. CWI plays an important role in two of them. In addition to these new initiatives and projects, CWI is, of course, still involved in the Bsik programmes BRICKS, MultimediaN and VL-e. On the international stage, CWI cooperates within ERCIM and W3C to put mathematics and ICT high on the agenda of the European Union.

Soon after CWI's move to Science Park Amsterdam in 1980, the present building rapidly became short of space. The problem could be temporarily solved by placing portakabins. However, we are very glad that NWO has now granted funds to permanently solve this problem. A new wing will add 4000m^2 to the current 6500m^2.

All of these items demonstrate our serious commitment to our mission – innovative fundamental research and the transfer of knowledge to society. We face an exciting future with numerous challenges and favourable prospects.

Jan Karel Lenstra
General Director

Overview

CWI Research Clusters

Probability, Networks and Algorithms (PNA)
1 - Algorithms, Combinatorics and Optimization
2 - Performance Analysis of Communication Networks
3 - Stochastic Dynamics and Discrete Probability
4 - Signals and Images
5 - Cryptology and Information Security

Software Engineering (SEN)
1 - Interactive Software Development and Renovation
2 - Specification and Analysis of Embedded Systems
3 - Coordination Languages
4 - Computational Intelligence and Multi-agent Games
5 - Distributed Multimedia Languages and Infrastructures

Modelling, Analysis and Simulation (MAS)
1 - Nonlinear PDEs: Analysis and Scientific Computing
2 - Computing and Control
3 - Nonlinear Dynamics and Complex Systems

Information Systems (INS)
0 - Standardization and Knowledge Transfer
1 - Database Architectures and Information Access
2 - Semantic Media Interfaces
3 - Visualization and 3D Interfaces
4 - Quantum Computing and Advanced Systems Research

CWI's mission and goals

For almost six decades the Centrum voor Wiskunde en Informatica (CWI) has been achieving high-quality research results in both theoretical and practical contexts. CWI is the national centre for mathematics and computer science in the Netherlands, founded just after World War II to contribute to the rebuilding of Dutch society. Ever since, CWI has had a keen eye for research based on societal needs and knowledge transfer. It is organized around research themes that are able to switch focus and goal. This enables CWI to be flexible while still obtaining thorough knowledge of specific research areas.

Human talent is the key factor in high-quality research. Over the years, CWI has educated many talented young people, of whom 110 men and 8 women now hold full professorships throughout the world. CWI provides these young people with ample opportunities to focus on research and develop their own direction. At this institute as well as at other knowledge institutions, universities, spin-off companies or industrial concerns, they can disseminate their knowledge and insights and with this contribute to the development of science and society.

CWI's mission is to perform frontier research in mathematics and computer science and to transfer knowledge to society. Its research policy comprises six goals:

1. To conduct advanced research of societal and scientific relevance
2. To act as a 'breeding ground' for academic staff
3. To train young researchers
4. To transfer knowledge to society
5. To play a leading role in the Dutch and European mathematics and computer science scene
6. To increase public interest in mathematics and computer science

1 To conduct advanced research of societal and scientific relevance

CWI's primary goal is to perform advanced research relevant to science and society. This can be seen from its main research topics: security, quality of software, societal logistics, scientific computing, quantum computing, earth and life sciences, database and Web technology and visualization. Success indicators are the number of scientific publications, the excellent performance judgment of the 2005 evaluation committee, and the numerous awards for CWI researchers, the most prestigious of which was the Spinoza Prize for Alexander Schrijver.

Prizes, decorations, acknowledgements and grants

Spinoza Prize for Alexander Schrijver

Alexander Schrijver has been awarded the Spinoza Prize 2005. He received this prize, sometimes called the Dutch Nobel Prize, for his outstanding, pioneering and inspiring research in the field of combinatorial optimization. Schrijver (1948) has been a researcher at CWI since 1989 and is a part-time professor at the Universiteit van Amsterdam. He has written two important standard books on combinatorics and algorithms. While writing these he filled in the gaps in the theory with new theorems and proofs, so that his field developed into a true discipline.

Mark Rutte, State Secretary of Education, presents the NWO Spinoza Prize to Alexander (Lex) Schrijver on 23 November in the Nieuwe Kerk in the Hague.

The Spinoza Prize consists of EUR 1.5 million – to spend on research of choice – and a statue of Spinoza. The Netherlands Organisation for Scientific Research awards the prize annually to a maximum of four scholars. Other winners in 2005 were René Bernards, Peter Hagoort and Detlef Lohse. Schrijver will spend the Spinoza Prize money on further research and the popularization of mathematics.

Sijbolt Noorda (Universiteit van Amsterdam) presents the royal decoration to Lex Schrijver.

László Lovász (Microsoft Research and Eötvös University) (left) and Paul Seymour (Princeton University) (right) pay a tribute to Lex Schrijver (middle) during the CWI Lectures 'Mathematics for Efficiency'.

Royal honour for Alexander Schrijver and Nico Temme

In addition to the Spinoza Prize, Alexander Schrijver has been decorated with the 'Ridder in de Orde van de Nederlandse Leeuw'. He received the royal honour on 19

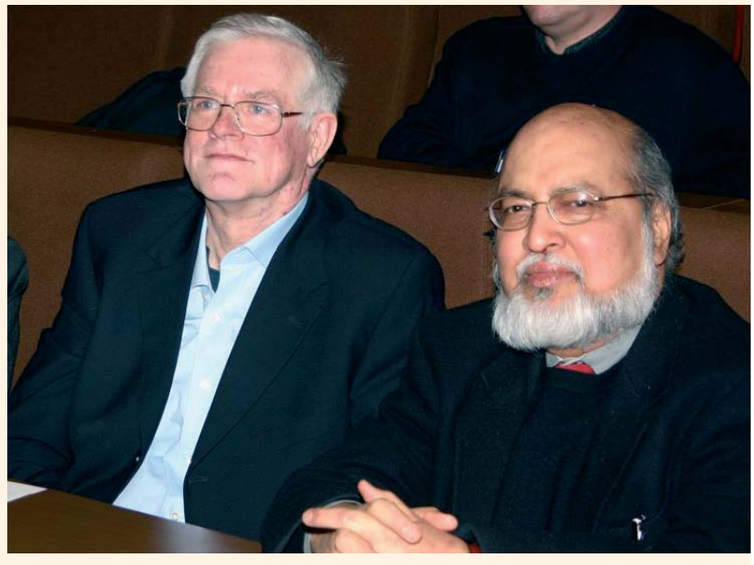
September from Sijbolt Noorda, President of the Board of the Universiteit van Amsterdam, for his excellent scholarship. This happened on the occasion of the first CWI Lectures – 'Mathematics for Efficiency' – organized for professor Schrijver upon his resignation as a member of the CWI Management Team and as leader of the research cluster Probability, Networks and Algorithms. Schrijver is continuing his work at CWI as a CWI Fellow, a position comparable to a university professor.

Nico Temme (1940) was appointed 'Ridder in de Orde van de Nederlandse Leeuw' for his achievements in the field of asymptotic special functions in mathematics and physics. He is a leading international expert in this field. After more than 37 years of service, Temme retired from CWI on 27 May. This was marked by the symposium 'From here to infinity'. During this Temme received his decoration from J. Streng, mayor of Abcoude. Streng read the appraisal from fellow scientists: "Temme is an influential mathematician, inspirator and cornerstone of CWI, a bridge between scientists and managers. He is an excellent ambassador for Dutch Science, of which your country can be proud". Temme is also editor and author of three chapters of the revised Handbook of Mathematical Functions, one of the most cited mathematical handbooks. It was originally edited by Milton Abramowitz and Irene Stegun and will now also be available on the Web with digital databases. After his retirement, Temme continues to work on this project.

Nico Temme receives the royal decoration.

Processes, terms, and cycles for Jan Willem Klop

"Since the 1970s the deepest and leading contributor to abstract rewriting theory has been Jan-Willem Klop," said Roger Hindley (University of Swansea, UK) one of the keynote speakers at the symposium 'Processes, terms, and cycles: steps on the road to infinity' held on 19 December. The symposium celebrated professor J.W. Klop's 60th birthday and the 25th anniversary of his connection with CWI. Arvind (MIT, USA) addressed the industrial impact of Klop. His theories are used by Bluespec Inc., which exploits the technology of chip design with term rewriting systems.
The technology is said to dramatically reduce code size and logic errors and it is under trial in a dozen companies. Klop is a researcher at CWI and the Radboud University Nijmegen and is professor of Applied Logic at the Vrije Universiteit Amsterdam.



Jan Willem Klop (left) with Arvind (Massachusetts Institute of Technology).

Van Dantzig Prize for Borst and Van der Laan

Sem Borst was awarded the Van Dantzig Prize on 11 April, for his pioneering work in statistics and operational research. The Dutch Association for Statistics and Operational

Research presents the award every five years to a young researcher who has a big impact on current developments in this field. The jury said: "Borst counts as one of the world's best young researchers at the edge of mathematics and communication systems. He has contributed much to the research on performance evaluation of packet scheduling, wireless networks, call centres and other means for efficient data communication." Borst works at CWI, the Technische Universiteit Eindhoven and Bell Labs in Murray Hill and received the prize together with Mark van der Laan of the University of California in Berkeley. This is the first time the prize was shared by two winners.

TT-Medal Project wins ITEA Achievement Award 2005

The Board of ITEA – Information Technology for European Advancement – selected the TT-Medal project as the winner of the ITEA 2005 Achievement Award. This was announced at the 6th ITEA Symposium in Helsinki, Finland, on 13 October. In this project researchers developed a standardized solution for software system testing, based on the TTCN-3 testing language from the European Telecommunication Standards Institute. They introduced it to the European industry. The outcome is a reduction in test development and test execution times and an improved product quality. Eleven participants took part in TT-Medal, including telecommunications manufacturers (Nokia, Nethawk and VTT Electronics), automotive manufacturers (DaimlerChrysler), transportation operators (ProRail), software test tool suppliers, software test consultancy firms (e.g., LogicaCMG), academia and research centres, such as Fraunhofer FOKUS, VTT and CWI's SEN2 research group.

Veni grant for fascinating quantum computing

NWO awarded CWI computer scientist Ronald de Wolf a Veni grant on 29 March. The researcher now has EUR 200,000 to spend on quantum computing research. Computers using quantum mechanical effects are more powerful than current computers. De Wolf will study new applications: not just methods for these futuristic computers but also the analysis of classical problems with quantum theory. The Quantum Computing and Advanced Systems Research group (INS4) is the first computer science research group to receive all three 'Innovational Research Incentive Scheme' grants from NWO: Veni, Vidi and Vici. In August 2004, Peter Grünwald received a Vidi grant for his research to improve statistical learning methods and in January 2004, Harry Buhrman received a Vici grant to strengthen his research group.

Veni grant for safer authentication with quantum cryptography

How can mutually distrusting parties communicate safely? On 20 December, NWO awarded a Veni grant to Serge Fehr for his research on information security using quantum mechanics. Fehr is researcher in the Cryptology and Information Security research group. Together with a group in Aarhus (Denmark), Fehr recently designed a new practical method for so-called Oblivious Transfer, which secures cooperation among mutually distrusted parties, such as possible partners in a company fusion. The basic idea behind the scheme is to swamp adversaries with more quantum information than they can possibly store.

Michael Schmidt, Jens Herrman (DaimlerChrysler), Erik Altena (LogicaCMG), Natalia Ioustinova (SEN2, Centrum voor Wiskunde en Informatica), Colin Willcock (Project Manager of TT-Medal, Nokia) at the 6th ITEA Symposium in Finland.

International evaluation committee: "CWI is a powerful and vibrant institute"

CWI rated 'excellent' in evaluation

'Excellent' is the rating CWI received from an international scientific evaluation committee. "The combination of mathematics and computer science and fundamental and applied research gives the institute a strong and unique position in the international research landscape," NWO reported. The committee emphasized that "CWI is a powerful and vibrant institute with a strong track record and a healthy future. NWO has every reason to be proud of CWI."

The evaluation committee members were Frank den Hollander (Technische Universiteit Eindhoven), Christopher Baker (University of Manchester), Susan Graham (University of California, Berkeley), Wendy Hall (University of Southampton) and Kurt Mehlhorn (Max Planck Institute for Computer Science, Saarbrücken). The international experts visited CWI in March, to look at past results, new developments and strategy. "Overall, CWI is a strong research institute with high-quality researchers working on highly relevant research themes," they said. The committee made several recommendations, for example, the formation of a scientific council, the formulation of a strategy for life sciences and reducing the autonomy of research themes.

The committee praised CWI's societal impact as a breeding ground for mathematicians and computer scientists for both academia and industry. The research fields have a heavy impact on other sciences. The committee defined the qualification 'excellent' as: "Work that is at the forefront internationally, and which most likely will have an important and substantial impact in the field. The institute is considered to be one of the international leaders." NWO subjected six institutes to an external evaluation: ASTRON, CWI, ING, NIOZ, NSCR and SRON. The evaluation takes place every six years.

The evaluation committee and CWI's management team, from left to right back row: Jan Verwer, Martin Kersten, Els el-Idrissi-Troost (NWO), Ron Dekker (NWO), Jan Karel Lenstra, Frank den Hollander (chair), Lex Schrijver, Paul Klint, Dick Broekhuis, front row: Christopher Baker, Wendy Hall, Foekje Grootoonk (NWO), Kurt Mehlhorn, Susan Graham.

Research

CWI's research is organized in themes. The pilot theme 'Convergent Media Infrastructures' received full theme status in 2005 and changed its name to 'Distributed Multimedia Languages and Infrastructures'. The group studies fundamental problems related to modelling, creating, encoding, and distributing media on a wide range of platforms and devices.

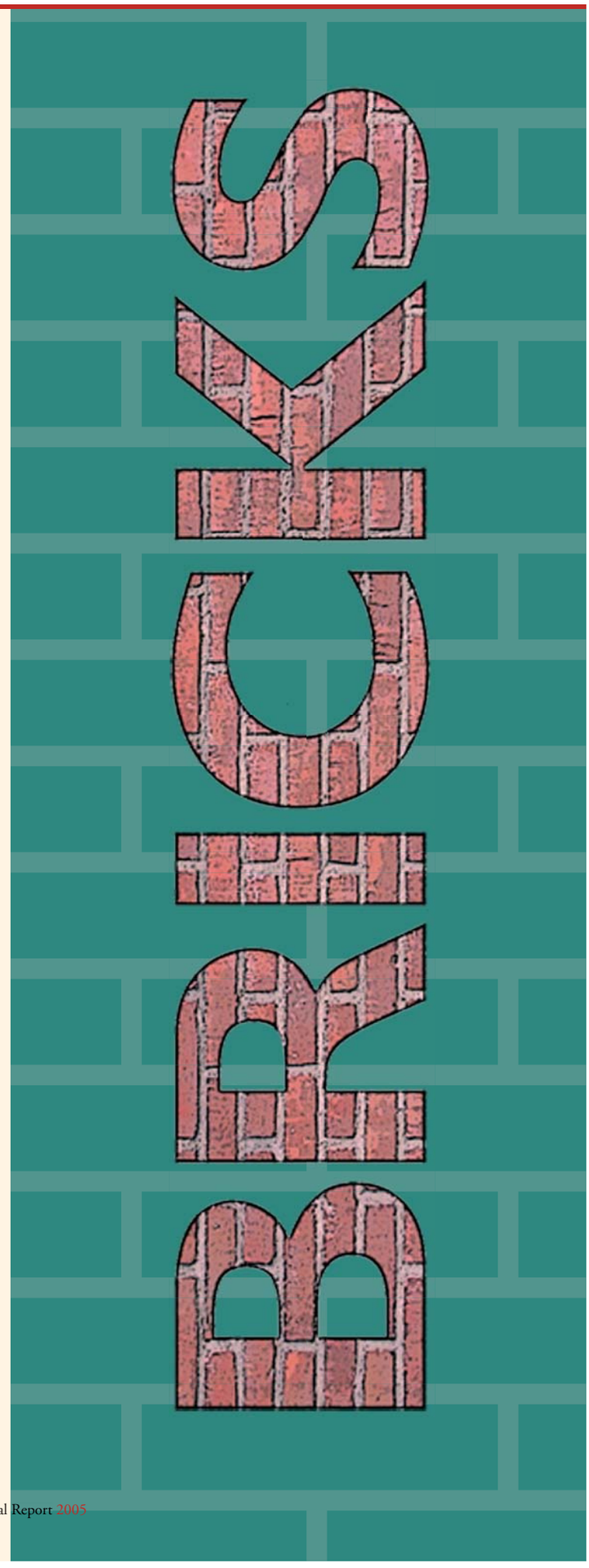
New research line life sciences for Science Park Amsterdam

Science Park Amsterdam has started a new research line on systems biology in the life sciences. Biologists, physicists, mathematicians and computer scientists will collaborate in this frontier research, to show how proteins, genes and other biochemicals cooperate in 'biomolecular networks' – chains of chemical reactions. Ultimate goal of this research is to understand how living organisms really function. Science Park Amsterdam has invested EUR 2.45 million in this initiative, realized with EUR 1.25 million from NWO and with resources from CWI, AMOLF and SILS (UvA). Results will have applications in public health and the food industry, such as rational drug design – designing medicines with effects that will be known beforehand – and improved food preservation techniques.

GLANCE, VIEW and FOCUS subsidies

NWO awarded 17 grants to four research programmes – CATCH, FOCUS, GLANCE and VIEW – to reinforce computer science in the Netherlands. CWI researchers coordinate three projects, each of which receives EUR 500,000. The FOCUS programme (Reinforcing Computer Science) stimulates fundamental computer science research. It is part of the Bsik programme BRICKS, developed by CWI and NWO. CWI Fellow Jan Willem Klop will interconnect and extend methodologies of formal methods, coalgebra and term rewriting. This theory might have applications in embedded software. GlobAl computer scieNCE (GLANCE) is looking for scalability of techniques for the next Internet generations. Farhad Arbab will develop a coordination model to control the quality of large-scale software applications. The Visual Interactive Effective Worlds (VIEW) programme stimulates visualization research. Robert van Liere will develop quantitative methods to evaluate virtual reality systems effectively.

The objectives of the new research programmes tie in with the goals of the NOAG-ict (new Netherlands' research agenda in ICT), presented on 5 July.



No innovation without fundamental knowledge

BRICKS programme boosts computer science research

Fresh knowledge, based on fundamental science to strengthen the country's economy cannot exist without innovation. Accordingly, the Dutch government has invested Bsik funds in the BRICKS – Basic Research in Informatics – programme (2004–2009), coordinated by CWI. BRICKS consists of several coinciding steps that reinforce each other: building competences, creating scientific output and transferring knowledge, and steered by questions from industry. The programme contains 12 projects and FOCUS – the Reinforcing Computer Science programme – coordinated by NWO.

Computer science research was strengthened with the filling of 32 PhD positions and 10 postdoc positions. These researchers produced 150 publications and contributed to conferences, workshops and symposia. They presented their first results on two BRICKS days, about scientific computing and the life sciences. BRICKS presented itself at several events: SIREN, the Sentinels Security event and the national 'Enlightening Science' congress (21 September). In April, the first research student partly financed by BRICKS – Willem Jan van Hoeve – received his PhD. His thesis 'Operations Research Techniques in Constraint Programming' concerned efficient optimizing methods for road logistics.

Input for the various projects came from the national NOAG-ict agenda, associate partners, the BRICKS Advisory Board and the ICT-Regie Outreach Office. This resulted in research on logistics with ORTEC, planning of rolling stock with NS/NSR Logistics, the allocation of flights to gates and of buses between gates and aeroplanes with Schiphol as a case study with NLR, flow-modelling problems for optimal ship design with MARIN, a C++ software prototype of the mobile channel middleware 'MoCha' with Almende BV, database research with Microsoft, Nedstat, navigation through panorama pictures with Cyclomedia, and biometrics research with Innovista. The BRICKS Advisory Board was enlarged with the appointment of W.H.A. Schilders of Philips Research in Eindhoven.

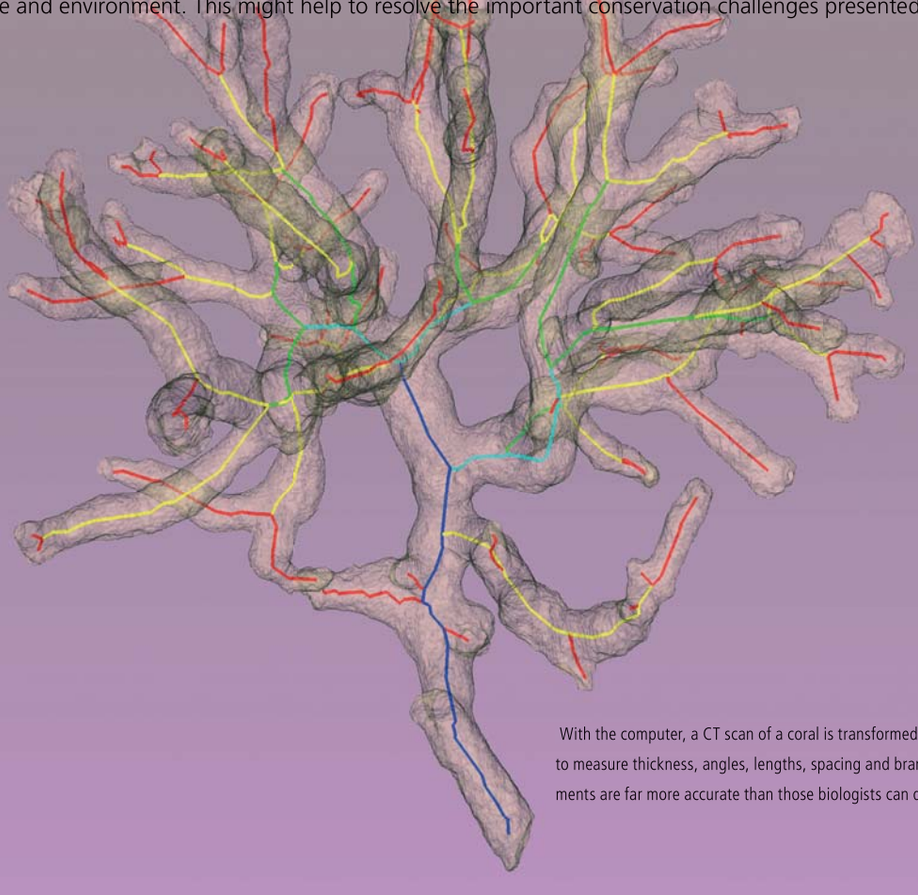
Computer measures coral structures

The Earth's coral reefs can only be conserved if biologists study them. CWI and the Universiteit van Amsterdam have developed sophisticated visualization methods to improve our ability to measure and analyse corals. These methods detect thickness, angles, lengths, spacing and branch ordering. This work was partly carried out in the Bsik Virtual Laboratory for e-Science project.

Coral reefs are important for both ocean biodiversity and the growing market of ecotourism. Corals exhibit a variety of forms. And under different environmental factors such as light, water flow and nutrients, the same species of coral can display quite different morphologies. Corals can, for instance, be spherical or branching. To compare and classify specimens, very precise measurements of thickness and branch distances must be made. Biologists used to do this by hand but this is time-consuming and error prone.

To make these coral measurements quicker, easier and more accurate, Krzysztof Kruszynski (CWI) and Jaap Kaandorp (Universiteit van Amsterdam) developed a method for quantifying the branching of coral shapes. Coral specimens are scanned in a CT scanner and the data are then filtered, segmented and transformed into a centreline skeleton. This simplifies feature detection. The computer then measures various attributes of the skeleton, such as thickness, angles, lengths and spacing of branches, and subjects the results to statistical analysis.

Despite problems like decayed coral parts and holes made by worms or human drilling, an easy and quick interactive visualization system has been created and is in use. In future, the researchers want to create more advanced result visualizations and quantify the accuracy of the computer measurements. Biologists can then study the correlation between shape and environment. This might help to resolve the important conservation challenges presented by coral reefs.



With the computer, a CT scan of a coral is transformed into a volume with a skeleton to measure thickness, angles, lengths, spacing and branch ordering. These measurements are far more accurate than those biologists can do by hand.

2 To act as a 'breeding ground' for academic staff

CWI is sometimes characterized as an ideal playground for researchers: Scientists do not have to educate master students at the institute – only PhD students – and qualified support staff relieve them from a number of managerial tasks. This policy results in a focus on scientific research, making CWI an excellent place to 'breed' academic talent. Over the years, CWI has educated many talented young people; 118 of them now work as professors all over the world.
In 2005 one CWI researcher Karen Aardal was appointed full professor and three other CWI scientists gave their inaugural speeches. Ronald Cramer was installed as a member of the Jonge Akademie, the younger part of the Royal Netherlands Academy of Arts and Sciences (KNAW).

Professors

CWI researcher **Karen Aardal** has been appointed professor of Combinatorial Algorithmics at the Technische Universiteit Eindhoven. She studies algorithms for combinatorial and integer optimization problems, such as frequency assignment problems in mobile communication and routing problems in logistics. In particular, she will try to strengthen the link between algorithms research in computer science and discrete optimization in mathematics. She is one of the few female professors in this field in the Netherlands. On 9 December, she gave her inaugural lecture: 'Een, twee ... ontelbaar' [One, two, ..., innumerable] about the complexity of optimization problems and the efficiency of algorithms.

Karen Aardal

Arie van Deursen gave his inaugural lecture 'The software evolution paradox' to mark his appointment as professor of Software Engineering at Delft University of Technology on 23 February. Our society increasingly depends on software. Software code should not only be designed but also constantly adapted to meet new requirements. However, changes mean more complexity. Eventually the software becomes so complex that updating is no longer profitable. This is called the evolution paradox. Van Deursen called for software exploration: Providing insights into the structure of existing programs so that software engineers are able to change the program more easily. This will extend the economic lifetime of software.

Arie van Deursen

What do diffusion, forest fires and mazes have in common? **Rob van den Berg**, head of the Stochastics research theme at CWI – addressed this subject in his inaugural speech 'Kans en Ruimte' [Chance and Space] as professor of Spatial Stochastics at the Vrije Universiteit Amsterdam on 15 June. The study of paths between pores in a gas mask – a random maze – led to the development of percolation theory some decades ago. Oded Schramm combined this with the theory of Brownian motion to calculate option values. Van den Berg will apply these new ideas to models of forest fires.

Rob van den Berg

Farhad Arbab gave his view on the flexibility of software during his inaugural speech 'Composition by interaction' at Leiden University on 28 October. Software is often composed of blocks, each of which describes a special functionality. Current models to build these blocks do not meet modern requirements. For instance, companies would like to compose their computer programs dynamically from independent subsystems and services. Arbab described his ideas for a compositional model for constructing complex systems out of simpler parts, using interaction as the most important concept.

Farhad Arbab

Scientific Meetings

CWI scientists were informed about their colleagues' work during several Scientific Meetings at the institute. Subjects varied from multimedia for the Semantic Web – a globally accessible representation of knowledge, and not just documents as is the case for the World Wide Web – to surprising proofs for mathematical problems with a theory that was originally designed for quantum computers.

Installation of the members of the Jonge Akademie, the younger part of the Royal Netherlands Academy of Arts and Sciences (KNAW) on 16 March. In front: Maria van der Hoeven, Minister of Education, Culture and Science; upper left, Ronald Cramer of CWI and Leiden University.

3 To train young researchers

PhDs theses

Eleven CWI researchers completed their PhDs in 2005. The subjects studied included optimizing methods for logistics, better software quality, faster and cheaper adaptation of source code, self-organizing behaviour, error-correcting codes for CD players, mathematics to describe axon development, investigating sparks, and the mathematics of curling cords. All of them benefited from the stimulating research environment provided by CWI.

Research Cluster Probability, Networks and Algorithms

Rachel Brouwer

Percolation, forest fires and monomer-dimers (or the hunt for self-organized criticality)
Vrije Universiteit, 6 October
Supervisor: Prof. J. van den Berg (CWI, VU)

Self-organization difficult to explain

Many physical objects and phenomena are similar on every scale. For example, regardless of how far you zoom in, the form of a snail's shell remains the same. Rachel Brouwer studied mathematical explanations of self-similarity, and focused on models of self-organizing critical systems. In critical systems, specific behaviour only occurs at a certain critical value of a parameter. For instance, water boils at 100 degrees Celsius. Self-organizing systems steer themselves to a critical state but the causes are often unknown. Self-organizing behaviour is associated with phenomena like forest fires, earthquakes, epidemics, sand dunes, evolution and the distribution of words in a text. Brouwer shows that in simplified models of forest fires large clusters of trees do not behave in a self-organizing manner but smaller ones do.

René Bekker

Queues with state-dependent rates
Technische Universiteit Eindhoven, 12 December
Supervisors: Prof. O.J. Boxma and Prof. S.C. Borst

Shorter waiting periods in queues using mathematical techniques

When employees have a lot to do for their clients, they work faster and faster. This cannot go on forever. When the workload is too high, their productivity can suddenly drop and the waiting lines rise. Classical mathematical models for waiting lines, such as clients in a queue or data in communication networks, used to consider productivity as a constant factor. René Bekker analyzed models to describe queues with productivity patterns that are not constant, but dependent on the state of the system. This has applications in production systems, water reservoirs and communication networks, where productivity depends on congestion in the network. Control takes place by admitting or refusing clients, depending on the workload at arrival, to maximize the long-term mean amount of work finished.

Rachel Brouwer

René Bekker

Dion Gijswijt

Matrix algebras and semidefinite programming techniques for codes
Universiteit van Amsterdam, 22 September
Supervisor: Prof. A. Schrijver

Error-correcting codes for CD players

Error-correcting codes are important for electronic data transfer. Small errors can occur when data is sent or saved, due to noise or damage of the medium. These codes can correct small numbers of errors using redundancy in the data: A CD with some scratches can still sound perfect. Dion Gijswijt studied the limits of the theoretically feasible quality of error-correcting codes.

Dion Gijswijt was part-time seconded at CWI (2002–2005).

Willem-Jan van Hoeve

Operations Research Techniques in Constraint Programming
Universiteit van Amsterdam, 19 April
Supervisor: Prof. K.R. Apt

Efficient optimizing methods for road logistics

How can several trucks deliver piles of packages to different places in the shortest possible time? There are many possible distributions of freight over the lorries, numerous potential routes for each vehicle, and the number of possible combinations grows exponentially. However, 'the shortest possible time' is a constraint that reduces the number of optimal solutions of this combinatorial problem. Willem-Jan van Hoeve applied efficient techniques from operational research – applied mathematics that helps with decision-making in real-life – to constraint programming in order to solve complex combinatorial problems. Van Hoeve used soft constraints (meaning 'rather not' instead of 'really not') and developed a method to efficiently minimize the total number of soft constraints for a sufficient solution to be obtained.

Willem-Jan van Hoeve

Research Cluster Software Engineering

Erica Abraham-Mumm

An Assertional Proof System for Multithreaded Java – Theory and Tool Support
Leiden University, 20 January
Supervisors: Prof. W.P. de Roever (Carl-Albrechts-Universität zu Kiel), Prof. J.N. Kok.

Erica Abraham-Mumm was seconded at CWI for one year during her PhD research. She described how properties of parallel Java programs can be derived with mathematical precision.

Miguel Valero Espada

Modal Abstraction and Replication of Processes with Data
Vrije Universiteit, 5 December
Supervisor: Prof. W.J. Fokkink, associate supervisor: Dr J.C. van de Pol

Better software quality with formal verification techniques

The quality of software components can be improved using formal verification techniques. This is particularly important for software in critical systems, such as air control systems. A small failure in these systems can cause huge financial losses or even loss of human lives. Verification techniques allow errors to be detected during the software development process. Valero developed a method to automatically compute a small scale-model of complex and large-scale systems that captures only the essential details. This technique is called abstraction. He proved that errors in the small scale-model are reflected in the real system, and vice versa. Researchers can now control larger systems than before.

Miguel Valero Espada

Jurgen Vinju

Analysis and Transformation of Source Code by Parsing and Rewriting
Universiteit van Amsterdam, 15 November
Supervisor: Prof. P. Klint, associate supervisor: Dr M.G.J. van den Brand

Faster and cheaper adaptation of source code with new language technology

Old source code can be adapted faster and cheaper to current demands by using generic language technology. This method can automatically handle tedious and elaborate tasks that maintenance programmers previously carried out by hand. Investing in software maintenance is attractive for companies since it is cheaper than developing new code. However, it is still expensive due to the vastness of the task: millions and millions of lines. In the past, the quality of systems to update software automatically was not high enough. With the new extensions of the technology, humans are still able to read and adapt the updated source code. Thanks to the lowered costs, Vinju sees opportunities for companies to do their own software maintenance, which has many advantages compared to outsourcing.

Jurgen Vinju

Peter Zoeteweij

Composing Constraint Solvers
Universiteit van Amsterdam, 29 November
Supervisors: Prof. K.R. Apt and Prof. F. Arbab

Efficient combinations for logistics

Many problems in daily life, science and industry are combinatorial problems, where a possible solution is based on a combination of choices influencing each other. An example is optimizing train schedules: Changing an arrival time of one train affects connections with other trains that in turn must keep good connections with even more trains. People quickly lose track and the number of possible solutions is often so high that even a computer cannot consider them all. Constraints – like 'transfer times must not be shorter than two minutes' – diminish the number of possible solutions. Peter Zoeteweij composed procedures to solve combinatorial problems – 'constraint solvers' – using available techniques. He sought the best combination of techniques for specific problems and demonstrated that his specialized newly-developed software produced useful and efficient constraint solvers.

Peter Zoetewij

Research Cluster Modelling, Analysis and Simulation

Johannes Krottje

On the numerical solution of diffusion systems with localized, gradient driven, moving sources
Universiteit van Amsterdam, 17 November
Supervisor: Prof. J.G. Verwer

Mathematician simulates axon development

How do neurons grow during the development of the nervous system in a foetus? Although several development principles concerning axons (the tips of the neurons) are known, the precise mechanisms are not. Axons grow towards higher concentrations of certain chemicals – guidance molecules. Johannes Krottje modelled this growth and made a flexible simulation package for biologists and brain researchers, called AGTools. It is one of the first simulation packages that allow scientists to study the growth of axons in a flexible way, with variable concentrations of guidance molecules and neuron locations. The goal of these simulations is to enhance insight in biological processes, reduce the need for experiments and improve the quality of the experiments still performed.

Johannes Krottje

Carolynne Montijn

Evolution of Negative Streamers in Nitrogen: a Numerical Investigation on Adaptive Grids
Technische Universiteit Eindhoven, 20 December
Supervisor: Prof. U. Ebert, associate supervisor: Dr W. Hundsdorfer.

Computer scientist investigates sparks with 'virtual microscope'

How are electric sparks formed? Carolynne Montijn developed a 'virtual microscope', a computational technique allowing her to zoom in and out on a spark while it moves. She used this in a computer model that provides highly accurate simulations of sparks. With this it was possible to quantitatively investigate the branching of sparks for the first time. The research can be applied in industry to clean gases and could increase our understanding of natural phenomena.

Carolynne Montijn

Robert Planqué

Constraints in Applied Mathematics: Rods, Membranes, and Cuckoos
Technische Universiteit Eindhoven, 7 April
Supervisor: Prof. M.A. Peletier, associate supervisor: Dr G.H.M. van der Heijden (UCL, London)

Mathematicians unravel curling cords

Curling telephone cords are an everyday phenomenon. Yet, one which is very difficult to describe in mathematical terms. Only closed rods like rubber bands could be described. In his dissertation Bob Planqué studied the behaviour of a curling rope with open ends by analyzing its energy minima. Since rods cannot self-intersect, the problem is very complex. Therefore, a special case of a rod on a cylinder was studied. Surprisingly, it seemed that, although the rope is lying along itself, forces are only transferred at certain separate points. Planqué also studied the mathematically related problem of lipid molecules forming membranes. This research opens the way for describing more complex situations, like DNA molecules.

Robert Planqué

4 To transfer knowledge to society

Since 1946, transferring knowledge to society has been one of CWI's key functions. Research results should not remain in the ivory tower of science but they must be used to strengthen our society. CWI has an active policy of licensing and creating spin-off companies. In 2005, negotiations started to realize the spin-off company Personal Space Technologies, with virtual reality applications. The E-Quality expertise centre for better quality of ICT services was started and a fast, open source database search system was launched.

Start of CWI spin-off Personal Space Technologies

'Just grab your molecule, galaxy, nucleus, CAD/CAM model or virtual prototype and explore it from all possible viewpoints.' This slogan comes from Personal Space Technologies (PST), a high tech spin-off company of CWI. PST is specialized in visualization and 3D interaction. One of its products is the Personal Space Station (PSS™), an affordable desktop interface that enables the user to work with multidimensional images and control them in an intuitive manner. PST products meet the high visualization and interaction standards of engineers and scientists. PST is funded by CWI Incubator and co-founders from Gallium Europe.

E-Quality expertise centre for quality of ICT services

With the fast-growing number of new ICT services and applications, it is becoming increasingly difficult to guarantee the required quality levels. E-Quality expertise centre was founded by CWI, TNO Information and Communication Technology and the University of Twente (UT), to strengthen research in the field of Quality of Service (QoS). The official launch took place on 30 September in Enschede. Two famous speakers closed the programme, James Roberts of France Télécom and Daniel Menascé of the George Mason University. Goals of the new centre are to transfer knowledge into society, to further expand the knowledge and expertise of the partners in joint projects and to train specialists. The participants bring in a wealth of expertise in the development of quantitative models and solution techniques, each with a different and complementary focus. E-Quality's expertise can help companies to develop and use high-performance ICT services in a cost-efficient manner.

During the kick-off meeting of E-Quality an agreement was signed by the directors of the participating institutes: Jan Karel Lenstra (CWI), Henk Zijm (UT), Gerard van Oortmerssen (TNO-ICT) and Peter Apers (UT-CTIT).

Launch MonetDB/XQuery

Computer scientists from CWI and the Universities of Twente and Konstanz launched the fast database search system MonetDB/XQuery at the Holland Open Software Conference in Amsterdam, on 1 June. Storing and querying high volumes of data in XML format – a relatively new standard for storing data – requires new software systems. MonetDB/XQuery is an open source system that provides a complete implementation of XQuery for the first time. XQuery is a query language to search XML data and this solution makes it possible to search both the content and structure of large XML documents. MonetDB/XQuery is built on the MonetDB Relational Database Management System developed by CWI. The new system performs better than any other current XQuery-system, both in terms of query performance and size of the queried documents. This was measured with the international XMark benchmark. The new XQuery processor can be used on a large number of hardware and software platforms – such as Windows and Linux – for scientific, commercial and private purposes. The research was carried out in the Pathfinder project of the Bsik research programme MultimediaN. For more information, see the research highlight article in this annual report.

Better methods to guarantee software quality

The complexity of software is increasing and at the same time its quality level is becoming more important: Safety-critical systems should never fail and commercial products have to perform well to keep the customers satisfied. Formal methods – types of mathematical descriptions – can be used to test and validate software and to prevent failures. This was the topic of the 4th International Symposium on Formal Methods for Components and Objects (FMCO 2005), held from 1 to 4 November at CWI.

Emergency Control

Formal methods are not only used to improve existing software but also in the development of new software with unexpected application areas. The CIM (Cybernetic Incident Management) Consortium applied these methods to emergency control: management of fires, floods and earthquakes with the aid of computer systems. The CIM Consortium consists of Almende, Cmotions, CWI, Delft University of Technology, Group 4 Falck and the Vrije Universiteit Amsterdam.

Development of ICT/New Media in Amsterdam

'The Amsterdam Innovation Motor' was the subject of a symposium organized on 23 November by Kenniskring Amsterdam (KKA) at CWI, in collaboration with Science Park Amsterdam. KKA is a 'knowledge circle' or network platform of more than a hundred companies, research institutes and governmental bodies in the Amsterdam region. Participants want to develop the Amsterdam knowledge economy, especially the three strong clusters ICT/new media, life sciences and sustainability. Job Cohen, mayor of the City of Amsterdam and chair of the KKA, opened the meeting. CWI gave a demonstration on 'New Media Distribution and Control: Producer and Consumer Issues'. The convergence of new media distribution channels, ranging from HDTV content over broadband Internet to postage-stamp size presentations on hand-held devices, has brought many problems to light. CWI theme leader Dick Bulterman highlighted work being done at CWI that could bring true innovation into media access and use.

PARTNERS IN RESEARCH

Companies

Almende
ASML
Backbase
Chipsoft
Cmotions
Conformiq
DaimlerChrysler
France Télécom
Groeneveld Groep
Group4Falck
IBM
Improve QS
Logica CMG
Lucent Technologies (Bell Labs)
Microsoft Research
Nokia
Oce Technologies
Philips
PinkRoccade
Post-Kogeko Transport Group
ProRail
Siemens
Software Improvement Group
SPSS
Stoneroos
Thales
Van Dale Beeld en Geluid
Verimag
Vos Logistics
…

(in total 50 companies)

Research Institutes

AMOLF
ESI
EURANDOM
Fraunhofer ICT Group
INRIA
MARIN
NIH (KNAW)
NIOZ
Telematica Instituut
TNO
…
(in total 39 research institutes)

CWI
Centrum voor Wiskunde en Informatica

Miscellaneous

NWO, STW, EU,
Min. Econ. Affairs, Min. Justice
Science Park Amsterdam
Dutch Research Schools
ERCIM: 18 members
W3C: 400 members
SARA, SURFnet
AMC, Rijksmuseum Amsterdam

Universities

Columbia University
Cornell University
Eötvös Loránd University
Erasmus Universiteit Rotterdam
ETH Zürich
Georgia Institute of Technology
Helsinki University of Technology
Hong Kong University
Imperial College London
Kyoto University
National University of Singapore
Moscow State University
Princeton University
Radboud Universiteit Nijmegen
Rijksuniversiteit Groningen
Saint Petersburg State University
Stanford University
Technische Universiteit Delft
Technische Universiteit Eindhoven
UC Berkeley
Université catholique de Louvain
Universiteit Leiden
Universiteit Maastricht
Universiteit Twente
Universiteit Utrecht
Universiteit van Amsterdam
Universiteit van Tilburg
Université Paris
University College London
University of Aarhus
University of Padua
University of Tehran
University of Waterloo
Vrije Universiteit, Amsterdam
…
(in total over 100 universities)

Based on the CWI Overview Research Activities 2005

Symposium IPR on software: the road ahead

Rejection of the proposed directive on computer-implemented inventions by the European Parliament means that fundamental questions about intellectual property rights (IPR) on software remain unanswered. CWI rekindled the debate with the symposium 'Intellectual Property Rights on software, the road ahead' held on 20 October for relations of CWI, as part of the annual 'CWI in Bedrijf' event. Over a hundred people from various organizations, from governmental bodies to law firms and software start-ups, attended the afternoon.

Software does not really fit into the copyright system, since copyright applies to precise formulations. Software code can easily be adjusted slightly without affecting how the program operates. A patent, however, deals with functionality: the idea cannot be copied. The difficulty with software patents is that they are often trivial. This also happens in other fields, as Paul Klint (CWI) showed in his example of a US patent on the comb-over hairstyle for bald men. Companies can hardly function if they adhere to all patents. Accordingly patents may counteract innovation, despite being necessary to make investments remunerative.

Jurist Robert Plotkin (Boston University, USA) proposed to shorten the terms for software patents to 2 – 3 years. One difficulty is that software varies from programs produced by teenagers in garages to code that costs millions of dollars. A lot of thinking has to be done about the various abstraction levels of software and its inventors: Can you register a patent if the software was not produced by a human being but by a genetic algorithm?

Yannis Skulikaris (European Patent Office) emphasized the innovative and technical aspects of patents. Roland Orre (Neurologic Sweden AB, Stockholm University) somewhat confused the public with a futuristic plan to use data mining and statistical methods to find holes in the current patent series that could be commercially exploited.

Panel discussion on IPR at the symposium, with Jan Bergstra (Universiteit van Amsterdam, Utrecht University), Robert Plotkin (Boston University School of Law), Roland Orre (Neurologic Sweden AB, Stockholm University), Lucy Guibault (Institute for Information Law, Universiteit van Amsterdam) and Yannis Skulikaris (European Patent Office, the Hague).

A panel discussion concluded the symposium. People from small companies told the public that they do not have resources for patents, so they have to count on company secrecy (black box software) and copyright. The fundamental question was raised: publish or patent? Jan Bergstra (UvA) suggested that patents are not so bad because they might force the industry to read scientific publications on software better. Skulikaris would like to see EU project reviewers around the table with IPR people.

CWI director Jan Karel Lenstra opens the symposium IPR on software: the road ahead.

Demonstration showing CWI results to visitors of the symposium.

Symposium on Embedded Software Quality

Together with Nokia and LogicaCMG, CWI organized the 'Symposium on Embedded Software Quality', sponsored by TestNet, on 31 August. Surprisingly few people in industry use standardized testing languages, although use of these methods could lead to greater profits. Speakers from CWI, LogicaCMG, Fraunhofer FOKUS, Testing Technologies, Philips, Confirmiq, Nokia Research Center and NetHawk explained more about their research projects and testing languages, such as TTCN-3.

CWI contributions to mobile multimedia standard SMIL 2.1

"CWI is proud to have contributed to SMIL 2.1", says CWI theme leader Dick Bulterman. The World Wide Web Consortium (W3C) released this version of the Synchronized Multimedia Integration Language on 13 December. With SMIL, authors can create interactive multimedia presentations and animations that integrate streaming audio and video with graphics and text. With SMIL 2.1, W3C is well on the way to making multimedia presentations on mobile devices a reality. Bulterman, head of the Distributed Multimedia Languages and Infrastructures group: "CWI's multiplatform implementation of the new features and profiles of SMIL 2.1 in the Ambulant Player has demonstrated the viability of the new specification."

Summer school for teachers

'The disk of five' was the subject of the annual summer school for high school teachers in Eindhoven on 26 and 27 August and at CWI in Amsterdam on 2 and 3 September. The participants learned more about the five mathematical topics Algebra, Analysis, Discrete Mathematics, Stochastics and Geometry, with lectures ranging from history – Christiaan Huygens in the 17th Century – to mathematical aspects of the World Wide Web. It was the last meeting for Jan van de Craats, who has successfully acted as scientific director of this summer school for the past seven years.

Jan van de Craats during a break at the summer school for teachers at CWI.

Coffee break during the Symposion on Embedded Software Quality.

5 To play a leading role in the Dutch and European mathematics and computer science scene

Focus and mass were major topics of the national ICT and mathematics agendas in the Netherlands. CWI was closely involved with the formulation of the NOAG-ict research agenda 2005–2010 and the formation of national mathematics clusters. Several conferences were organized and scientific communities were supported. On the international stage, the promotion of computer science and mathematics in the European Union was reinforced.

NOAG-ict agenda

The NOAG-ict research agenda 2005–2010 is a national strategy document for ICT research in the Netherlands, formulated to make the most of the opportunities that Europe, economics, society and science offer. This is done by stimulating research and clarifying the structure of ICT research in the Netherlands. Promising innovative research trends were combined into nine appealing ICT research themes, both risk-taking fundamental science and applied research. The formulation of this agenda was coordinated by the Informatica Platform Nederland (IPN), with CWI cluster leader Paul Klint as its chairman, the Dutch Technology Foundation (STW), and the Netherlands Organization for Scientific Research (NWO). CWI is also involved in ICTRegie, established by the Dutch government to stimulate the innovative possibilities offered by ICT research in the Netherlands.

Mathematics clusters

At the same time, Dutch mathematicians from universities, institutes, and research schools, sought ways to structure and cluster their research, so as to stimulate Dutch mathematics research and improve its interaction with society. This is important for the Netherlands, since mathematics is not only a science in its own right, but it also supports other research disciplines and is extremely helpful in commercial processes. Three national research clusters were selected in 2005: 'Discrete, Interactive and Algorithmic Mathematics, Algebra and Number Theory' DIAMANT, 'Nonlinear Dynamics of Natural Systems' NDNS and 'Fellowship of Geometry and Quantum Theory' GQT. CWI plays an important role in both NDNS – of which CWI researcher Arjen Doelman is the chairman – and DIAMANT. The clusters are characterized by multidisciplinary collaborations and they might play an important role in future master education programmes.

Cream of Science

Ten members of CWI's staff were invited to join the 200 Dutch top academics whose oeuvre of publications were made publicly available by the national project Digital Academic Repositories (DARE). On 10 May the president of the Netherlands Academy of Arts and Sciences (KNAW), Frits van Oostrom, launched the creamofscience.org website. DARE aims to encourage institutional repositories to make the scientific output of all Dutch scientific organizations available digitally and according to the international Open Archives Initiative (OAI) protocol.

World Wide Web Consortium

In the World Wide Web Consortium (W3C), researchers, companies and governments cooperate to develop Web standards. W3C has about 400 member organizations from over 40 countries. CWI is not only an active member in several working groups, but also manages the regional W3C Benelux Office. To disseminate knowledge, the office organized two tutorials in Antwerp (Belgium) in cooperation with the Internet Society Belgium. On 16 February, Ivan Herman (W3C/CWI) spoke about Semantic Web Technologies. Semantic Web is one of the most important activities of W3C. Its aim is to create a universal medium for exchanging data across application, enterprise and community boundaries. CWI researcher Steven Pemberton gave a tutorial on XHTML2 and XFORMS on 3 October, as chair of the XHTML and XFORMS working groups. On 3 June several CWI/W3C researchers visited the 10th anniversary of W3C Europe, which was celebrated at Science Park Sophia Antipolis in France.

Conferences, seminars and workshops

CWI (co-)organized several conferences and seminars to support scientific communities and knowledge exchange. For example, ICME 2005 (IEEE International Conference on Multimedia & Expo) in Krasnapolsky, Amsterdam from 6 to 8 July, the NTVI Theory day for computer scientists in Utrecht on 4 March, and together with NWO the workshop 'Robust Numerical Methods for Singularly Perturbed and Multiscale Problems' on 3 and 4 November. From 9 to 13 May CWI co-organized a workshop in the Lorentz Center in Leiden on spark formation and lightning. From 7 to 11 November scientists from different specializations and

ERCIM

CWI director Jan Karel Lenstra was elected vice president of ERCIM, the European Research Consortium for Mathematics and Informatics. The consortium has 18 institutional members and over 10,000 computer scientists and mathematicians. It was established in 1989, with CWI as one of the three co-founders. In 2005, its new strategy was formulated. "ERCIM wants to contribute to a leading role of Europe in ICT by promoting cooperation in research, technology transfer, innovation and training. This will create added value for its members, for their countries and for Europe". In 2005 the EU asked ERCIM for advice on its project 'Beyond the Horizon' to identify the emerging grand challenges for the future, especially for the forthcoming 7th Framework Programme. Several CWI researchers were involved in the brainstorming workshops.

ERCIM's research is done by working groups and CWI participates in nine of them. The ERCIM Working Group on Image and Video Understanding, lead by CWI researcher Eric Pauwels, received the ERCIM Working Group Award 2005 in Helsinki on 30 May. "This was clearly the most outstanding group due to their successful Network of Excellence proposal - MUSCLE - and the large amount of joint activities that resulted from this," the jury said. The group received EUR 20,000 and spent the money on exchange visits to start new research collaborations. In his speech, Eric Pauwels paid tribute to the late ERCIM President Stelios Orphanoudakis, who invited Pauwels to consider the possibility of setting up the working group.

ERCIM president Keith Jeffery (CLRC, UK) hands the ERCIM WG Award 2005 over to Eric Pauwels (CWI), leader of the winning Working Group on Image and Video Understanding.

countries also gathered at the Lorentz Center for a workshop on complex pattern formation. A cardiac arrest, a flash of lightning and the reproduction of bacteria have much in common: All these processes involve pattern formation. This workshop marked the launch of the NWO programme 'Dynamics of Patterns'.

The 2005 Conference of the Dutch-Flemish Numerical Analysis in Zeist (12 to 14 October) was organized by CWI for about 100 people, 40 of whom were PhD students, to stimulate contacts between numerical mathematicians in the Netherlands. Together with Richard. Gill (Utrecht University) and Mike Keane (Wesleyan, Connecticut) CWI organized the annual national Stochastics Meeting in Lunteren from 14 to 16 June, with eminent international speakers, such as David Gilat (Tel Aviv) and Marc Yor (Paris). The mathematics community highly values this meeting, as shown by its many sponsors: NWO Research Council for Physical Sciences, the Netherlands Society for Statistics and Operations Research (VVS), the Mathematical Research Institute (MRI), and the Thomas Stieltjes Institute for Mathematics.
CWI supports the Royal Dutch Mathematical Society (KWG), by sponsoring the electronic newsletter and by supplying the scientific secretary of the board.

A Dutch-Belgian Database Day was organized at CWI on 31 October to train young researchers in database research. PhD students and postdocs presented their results, for instance in the field of digital forensics. Connected to this event was the Third Workshop on Ambient Databases on 1 November, where results of the AmbientDB project were discussed. This project is part of MultimediaN in which many Dutch scientific, commercial and societal institutes are cooperating to further develop multimedia technology and its applications. The workshops were organized by CWI and the University of Twente, under the auspices of SIKS, the Dutch research school for Information and Knowledge Systems.

During the Stieltjes Afternoon at CWI on 15 September, Marc van Raalte (CWI) received the Best PhD Thesis of the Year Award from the Stieltjes Institute for Mathematics, for his thesis 'Multigrid Analysis and Embedded Boundary Conditions for Discontinuous Galerkin Discretization'. His work led to six articles in international journals and interest from foreign organizations, like NASA. The prize consisted of a certificate and EUR 1200.

Jan Karel Lenstra congratulates Marc van Raalte with the Best PhD Thesis of the Year Award.

Minister Laurens Jan Brinkhorst of Economic Affairs (right) and Amsterdam alderman Laetitia Griffith (left) visited Science Park Amsterdam on 12 September.

6 To increase public interest in mathematics and computer science

CWI shows the fun side of science to make people enthusiastic for computer science and mathematics. It collaborated in the 'Science Unlimited' week at Science Museum Nemo and in two performances of science theatre Adhoc. Fifteen press releases for the media were sent out and the national press reported about CWI research on several occasions. A new series of semi-popular lectures was started: the CWI Lectures. Further, CWI sponsored Vierkant voor Wiskunde, an organization mainly targeting to stimulate teenagers' enthusiasm for mathematics.

Science Unlimited

Hundreds of excited children watching thunder and lightning movies, and yelling loudly when one of their friends generated large sparks with a special bike: This was the impression of CWI's demonstrations at Science Unlimited. This week, from 15 to 19 June, was dedicated to physics and organized in Science Museum Nemo in Amsterdam during the World Year of Physics. Professor Ute Ebert and Carolynne Montijn explained the origin of electricity, lightning and sprites – extraordinary lightning above the clouds – in cooperation with science theatre group Pandemonia. Many people lingered around the speakers afterwards with questions. Since the youth shapes the future, the researchers were very pleased with this enthusiasm for science.

Carolynne Montijn at the lightning show in Science Museum Nemo.

Science Theatre Adhoc

Ute Ebert was also present at the performance 'Searching the wondrous world of genes and proteins, nanos and neutrinos, bits and bytes, cetas and teras' of Science Theatre Adhoc on 30 September, in Eindhoven. Lex Schrijver took part in the same performance in the former accelerator building at

Theatre Adhoc
Ute Ebert

Theatre Adhoc
Lex Schrijver

© pictures: Hannie van den Bergh / Theater Adhoc

the Science Park Amsterdam on 7 October. The 'narrative documentary theatre performance' combined science with movies, cabaret and questions, particle physics and travel stories. CWI scientists participated in an interesting interview about their research.

Google teaches computers the meaning of words

One of the CWI news items in the media was about computers learning the meaning of words with the help of the Google search engine. CWI researchers Rudi Cilibrasi and Paul Vitányi found a way to use the World Wide Web as a massive textbook for computers and published this in New Scientist in January. A word's meaning can often be derived from neighbouring words. Two related words are likely to give more hits when plugged into Google than two unrelated words. Cilibrasi and Vitányi developed a statistical measure of the 'distance' in meaning between words, based on the number of Google page hits. The lower this so-called normalized Google distance, the more closely words are related. In this way maps of words can be generated, which the computer could use to learn their meaning. The method can, to a certain extent, distinguish between colours and numbers, between primes and composite numbers, and between 17th century Dutch painters. The researchers got an 87.5 percent mean agreement with expert-entered semantic knowledge in WordNet. The method was also able to do a simple automatic translation.

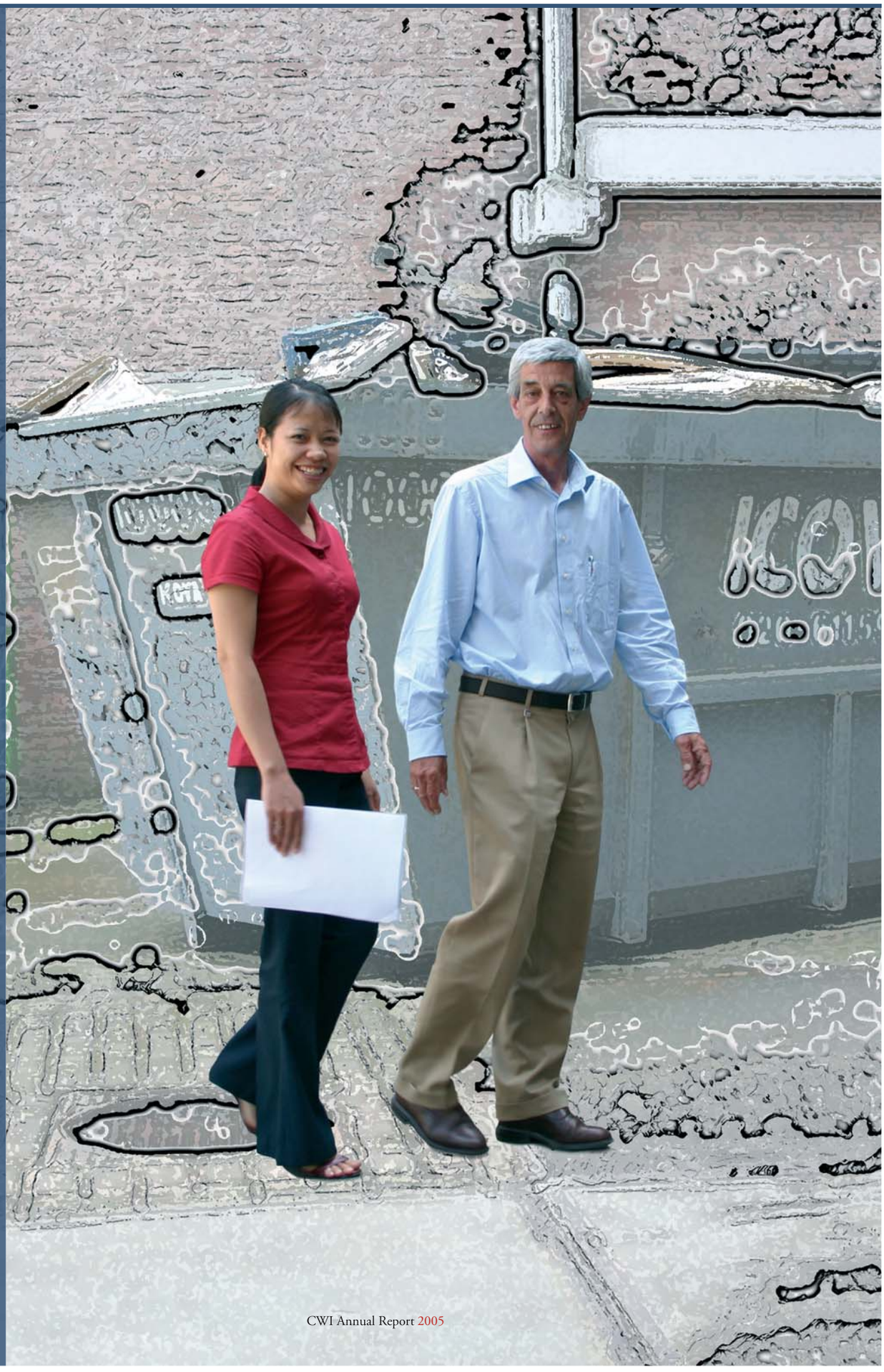
Lectures

Several CWI scientists gave lectures for non-scientific audiences. Paul Klint spoke about 'Software as a box of building blocks!?' during the Impetus Lecture at the Hogeschool van Amsterdam on 21 December.
Harry Buhrman gave a Paradiso lecture on 3 April, 'Quantum computers, computers that think differently'. Quantum computers use the fact that a quantum particle can be in several states at the same time. Will the new generation of computers be infinitely powerful and fast? Paradiso lectures are organized by the K.L. Poll-stichting, NWO, Dutch broadcasting corporation VPRO and Paradiso in the Paradiso concert hall.

Science Day

Over four hundred children and adults visited CWI during the annual Science Day of the Science Park Amsterdam. In the science café in the CWI Library visitors could join mini classes on whale tails, renovating software and powerful quantum computing, while enjoying some drinks. Outside CWI the Dutch youth juggling champion gave a workshop with mathematical comments from a scientist. People splashed water while trying to solve IQ test problems, like: If you have two buckets of 3 and 5 litres, how can you measure 1 litre? Girls and boys enjoyed the Pretlabs (fun labs) where they could make electronic toys and gadgets. This year's national theme was 'Know your forces'. Mathematical games to measure brain power were demonstrated by Pythagoras, Vierkant voor Wiskunde and Arabesk. Dancing theorems, an auction game and interesting demonstrations – like visualization of cancer research – gave an impression of CWI research. Ute Ebert's flashy lightning show concluded the day.

Research Highlights



Mathematics discovers unexpected change in plankton populations

CWI models predict plankton oscillations in deep ocean layers

Will there be enough plankton left to feed shrimps and whales if the climate changes? This question arose when mathematicians from CWI and biologists from the Universiteit van Amsterdam and the University of Hawaii (USA) modelled plankton growth in deep water layers of the oceans, formerly assumed to be stable. Surprisingly, plankton concentrations appeared to oscillate – varying from enormous quantities to almost nothing – when temperature rises. These unexpected results, found in 2005, were published in Nature on 19 January 2006.

Phytoplankton

Plankton forms the basis of the food chains in the oceans. Clouds of plankton can be observed as coloured shades drifting in the water, but individuals are too small to be seen without microscopes. Plankton is found in two forms, animals and plants. Phytoplankton is plant-like and it consists of hundreds of thousands species of algae. Just like trees and plants, they obtain their energy by photosynthesis, using sunlight, and by nutrients from the water. Phytoplankton influences both the marine food web and the climate: During photosynthesis, it absorbs the greenhouse gas carbon dioxide. Because the oceans cover roughly 70% of the earth's surface, marine phytoplankton is quantitatively important for reducing the greenhouse effect.

Food and light

Many phytoplankton species sink, so in order to catch sunlight they depend on upward currents to lift them. Other species float by means of gas bubbles in their interior. Their nutrients – such as nitrate, phosphate, and even iron – are relatively abundant in the lower, darker regions of the oceans. This water slowly mixes upwards with warm water at the surface, where sunlight falls in. Most phytoplankton can be found in a region where there is enough light and food to keep a population alive, approximately at a 100 metres deep. Satellites monitor phytoplankton concentrations carefully, but only to a depth of about 20 metres – below that it is too dark.

Warm and cold

The water temperature in the oceans is vital for plankton growth. Swimmers in the sea can feel sudden differences in temperature between layers of warm and cold water. Similarly, oceans also have relatively stable layers of warm and cold water, mixing slowly. This is called vertical stratification and is a widespread phenomenon in the oceans. A larger temperature difference reduces the mixing of water and consequently the upward transport of plankton food. Global warming due to climate change thus implies less upward mixing of nutrients in the oceans.

Surprising effects

What effect could this have on plankton populations? This was investigated by biologist Jef Huisman of the Institute for Biodiversity and Ecosystem Dynamics (IBED) of the Universiteit van Amsterdam and mathematicians Nga Pham Thi and Ben Sommeijer of CWI. They developed advanced computer simulations to study how reduced upward mixing of nutrients affects the growth of marine plankton. Surprisingly, these simulations predicted that plankton populations will show strong oscillations and even chaos when this happens, see Fig. 1. This may have a negative impact on the food chains of the oceans and on the uptake of the greenhouse gas carbon dioxide into the oceans. On the other hand, it has a positive effect on the number of plankton species and thus on the biodiversity of the ocean.

Mathematics

The mathematics behind these new predictions is based on a simulation of plankton and nutrients dynamics. The model consists of a set of mathematical equations, of the 'integro-partial differential equations of advection-diffusion-reaction' type. These equations are relatively difficult to solve due to mutual dependencies ('coupling') of plankton species, which all compete for light. Further, the plankton quantity depends on the penetration of light into the water. The light intensity at a certain depth not only depends on the incident light at the water surface, but it is also subject to absorption by photosynthesizing phytoplankton. So, more light implies plankton growth, consequently more photosynthesis, more absorption and thus less light. The solution of the equations had to be calculated numerically – after many advanced mathematical operations – by approximating the solution in hundreds of points. Computational advances increasing the efficiency of numerical solutions were essential to analyze the intriguing fluctuations in the phytoplankton.

Ocean measurements

The model predictions were rather unexpected, because they contradicted the conventional wisdom that deep plankton in the oceans would be stable. Therefore, the scientists compared their model predictions with data from long-term plankton measurements in the subtropical Pacific Ocean (see Fig. 2), carried out by David Karl of the University of Hawaii. This part of the ocean is strongly stratified, with a low supply of nutrients into the surface layers. Phytoplankton indeed exhibited complex population fluctuations, consistent with the computer predictions. These results were published in Nature (19 January 2006) in the article: Reduced mixing generates oscillations and chaos in the oceanic deep chlorophyll maximum.

The Netherlands Organization for Scientific Research (NWO), the Dutch Bsik/BRICKS project, the American National Science Foundation (NSF), and the Gordon and Betty Moore Foundation supported the investigations.

Figure 1

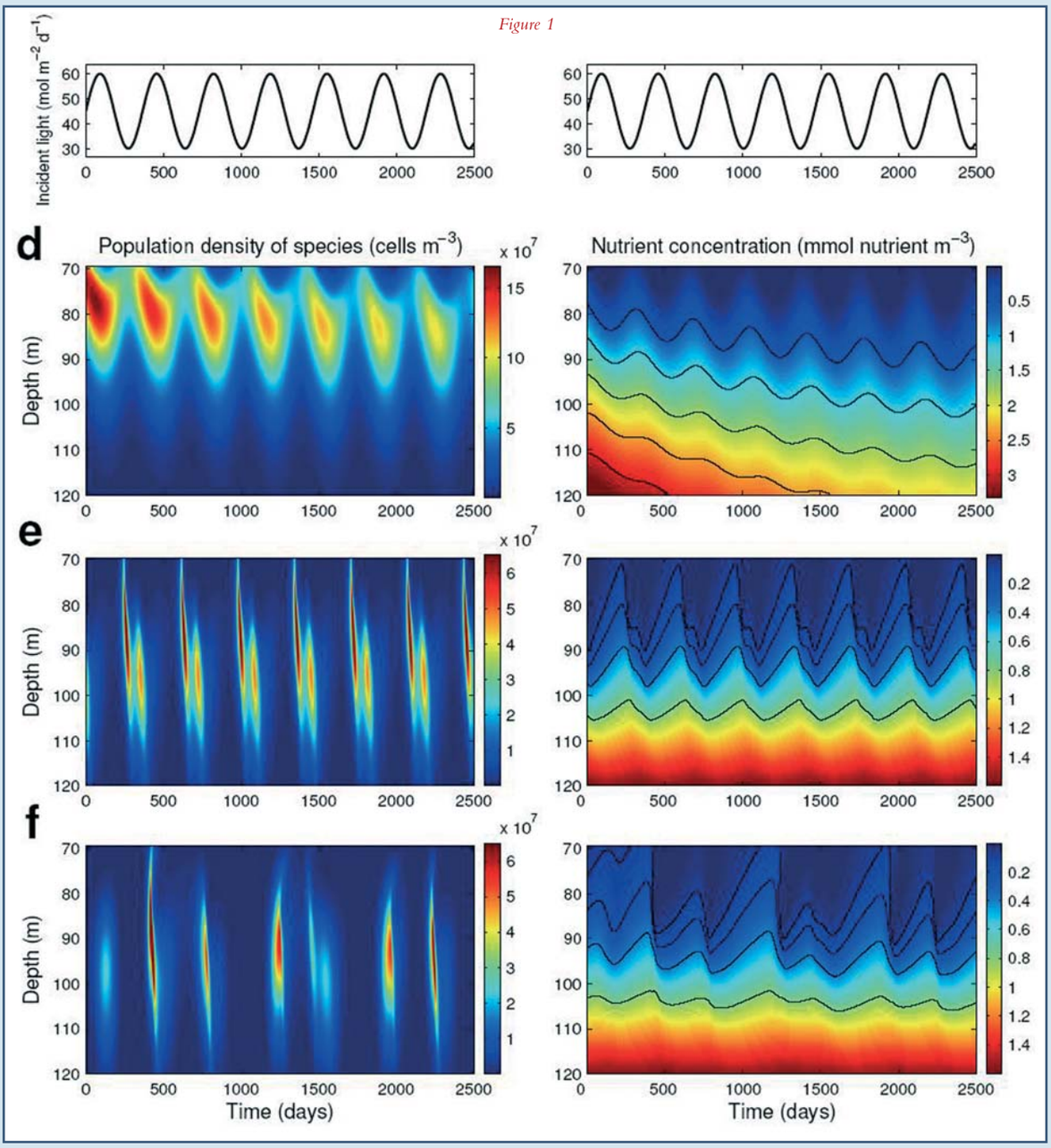


Figure 1: Model simulations at different vertical mixing rates, left showing plankton dynamics and right the nutrients. The top panel of figure 1 (well mixed situation) shows that the deep chlorophyll maximum is following the seasons. The following panels display the effects of global warming. The middle panel (moderate mixing) shows double periodicity in a seasonal environment. The lower panel (low mixing) shows chaotic behaviour. Illustration: redrawn from Huisman et al. 2006, with permission from Nature.

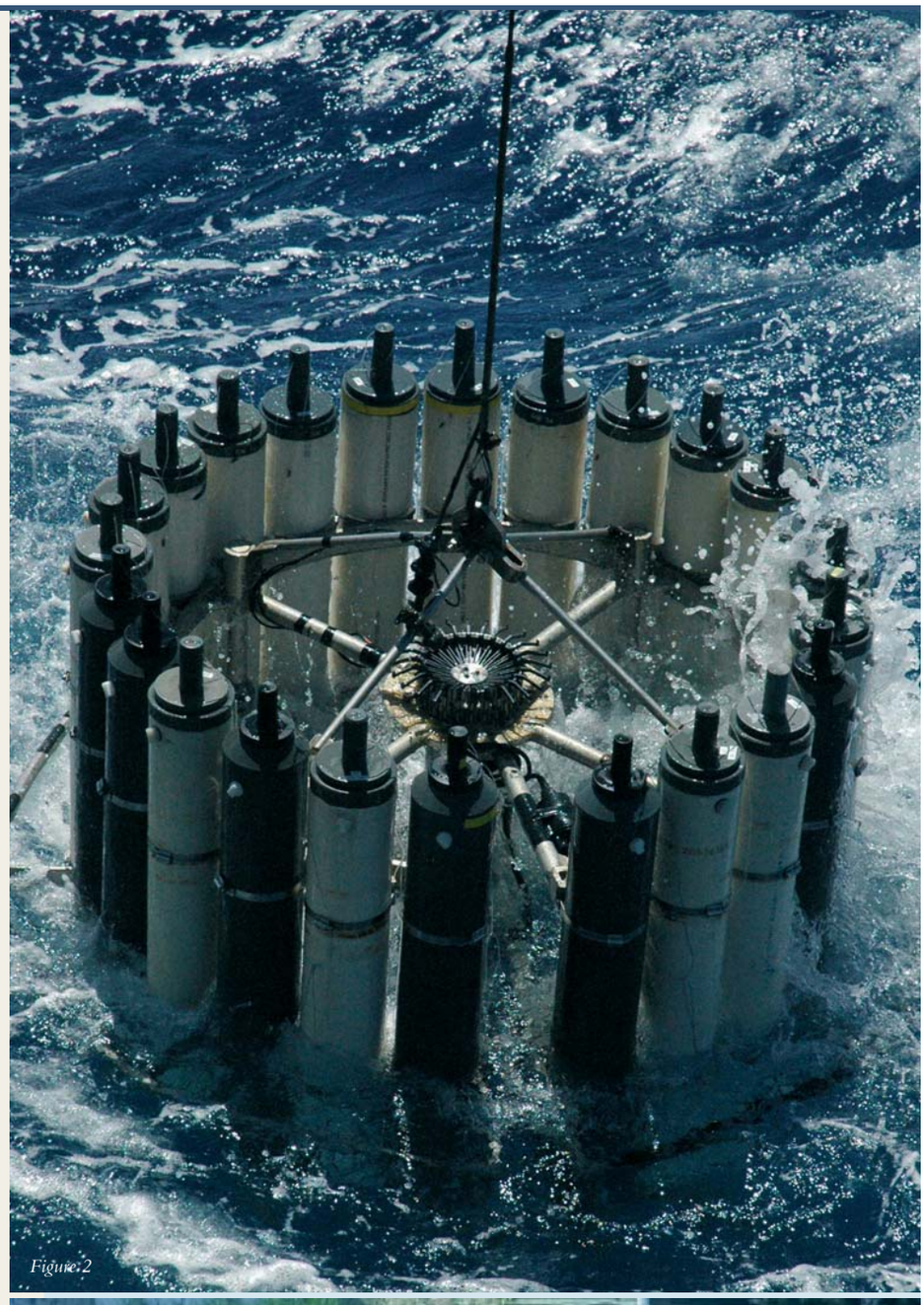


Figure 2: Taking a plankton sample in the waters near Hawaii.

Figure 3: CWI had experience with modelling algae: In 2003, they modelled the concentration of the poisonous blue alga in the Nieuwe Meer (The Netherlands) in case warm summer water was aerated by a system of underwater tubes on specific depths.

Links: http://www.cwi.nl/projects/pdels/Phytoplankton/

Coordination of emergency communication in safe hands

Evening, 15 July 1996: A Belgian Hercules airplane crashes at Welschap Airport near Eindhoven, the Netherlands. Firemen extinguish the fire, unaware of the fact that over forty people are still inside. Thirty-four people do not survive. This is a sad example of human communication that went wrong in moments of stress. Would an automatic communication system have detected that essential information was missing? Within the Cybernetic Incident Management (CIM) project, CWI collaborates with universities and high-tech companies to improve communications in emergency situations.

Disaster management

Formerly, disaster management was all about knowing contingency plans – mostly formal and legal rules – by heart. Nowadays, a more active approach is needed by performing realistic simulations in practical exercises. During these trainings it often appears that communication is the bottleneck in disaster management. Reason for high-tech company Almende to investigate whether its ASK system could also be applied to emergency control. This system was originally designed for dynamic resource planning, communication and distributed knowledge management.

The ASK system itself is based on a set of intelligent agents: autonomic pieces of software that collaborate to fulfil a certain task. For instance, if 10 volunteer firemen are needed the agents in the system know who is on duty to form this team and whom to call if some of them cannot be reached or are otherwise unavailable. It calls people through their preferred communication medium, such as analogue or ISDN telephone, GSM, VOIP, SMS or e-mail. It can scale-up and escalate a situation according to the communication protocol. It searches the best solution and after the call, it asks for feedback in order to improve itself. Many test scenarios are provided. It takes care of the complete communication coordination.

Human factor

Are people willing to use this futuristic automatic incident management system? Would they feel safe to place communication coordination in the hands of invisible and impersonal software agents? The system has several benefits, Peet van Tooren of Almende shows. It is more consistent and reliable than human beings in stress situations. Workers are often closer to a disaster than a coordinator, so precious time could be saved (and some 'filtering problems' avoided) if their first hand information could automatically be dispatched to the appropriate people involved. Despite all benefits, trials to experiment with it encountered some opposition in governmental organizations. Why change a safety-critical system that works well, at least most of the time?

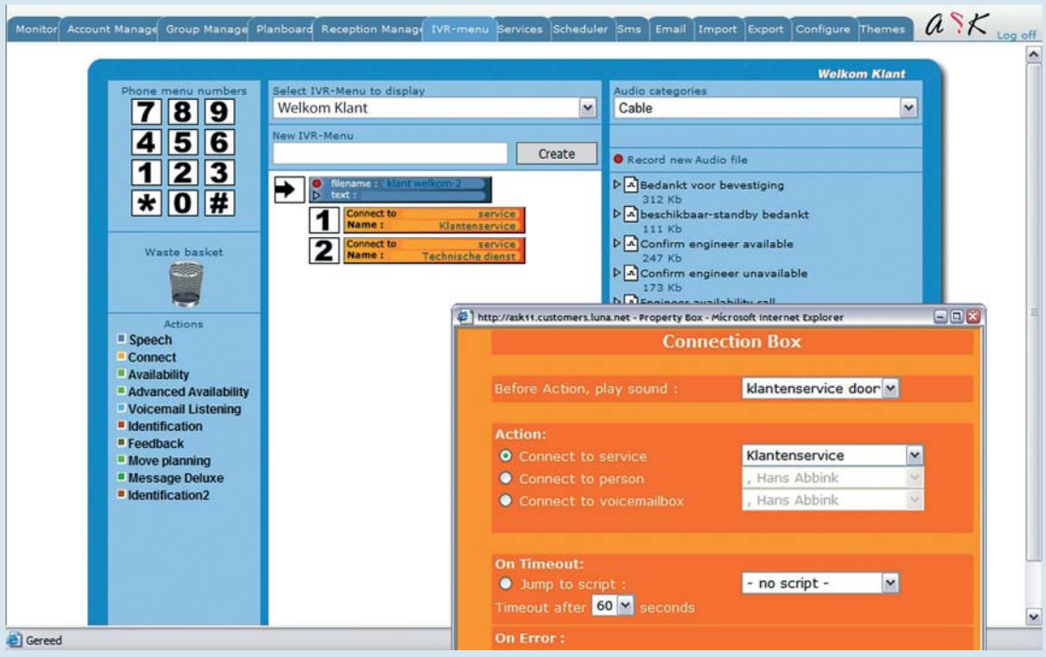
Garden hose

For Almende, slight disappointment was no reason to stop further product improvement. One class of improvements in the ASK system uses the concept of mobile channels developed by the SEN3 research group at CWI. A mobile channel in software can be compared with a garden hose, Farhad Arbab, researcher at CWI and part-time professor at Leiden University, explains. If person A shouts a message in one end of the hose, person B could hear at the other side what has been said. If B passes the hose to person C, A does not notice the difference and the message will not be affected either. This quality can be extremely helpful in real life situations. For instance, if you need person B but he is on holiday or he is not the right person to answer your question, you will immediately be connected to C, without even noticing the change.

The concept of mobile channels presents a real change in the ideas of building modern software systems. The essentials are not about pieces of software anymore, but about programming the communication and coordination between them. Farhad Arbab foresees big advantages for Service-Oriented Computing (SoC), where composition of existing services can be offered as a new service. Consider tourism as an example, where existing reservation services from different organizations (car rentals, hotels, airlines) can be composed to one new service. With current technology, construction of a composed service is far from trivial and is only possible if provisions have already been made in the existing to-be-composed services.

Infrastructure

With mobile channels independent organizations can set up new businesses that do not require alterations to existing services. The crucial point is that mobile channels offer a mechanism to fully decouple software behaviour from its underlying code. Mobile channels only know dynamic connections: They determine which software module is connected to the others, and when. This becomes indispensable when each concern falls within the jurisdiction of an inde-

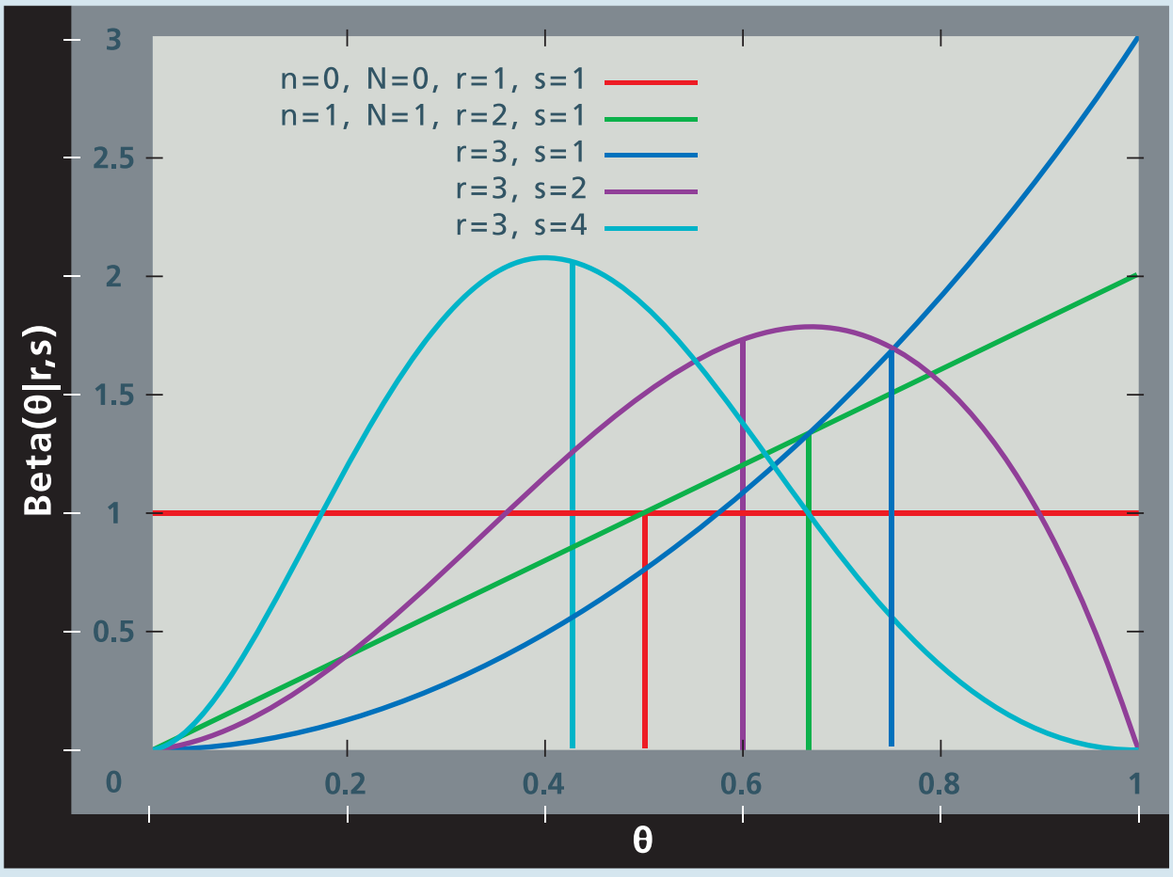


Almende's ASK system

pendent autonomous organization, as is the case in incident management. CWI's Reo system implements communication and coordination protocols that regulate, synchronize, and combine the data streams through mobile channels. If one volunteer fireman cannot assist at a certain moment, the protocol can have the system switch to a neighbouring fire department, without the involvement or knowledge of the fireman or his fire department. The SEN3 research group provides the infrastructure with which these communication systems can be built.

Reliability

Another contribution to improve intelligent communication systems comes from the SEN4 research group at CWI. Here reputation management is studied, as applied to software agents. Just like human beings, each software agent has its own interests. It would be of great help to know how reliable a software agent is before doing business with it, or to know if a human worker can be trusted to appear at work in time.



Computations of reputations, based on positive (r) and negative (s) experiences. The graphs represent probabilities of reliability. The purple line describes a reliable agent while the light blue line depicts a less reliable agent. Easy calculations can be done with the expected values, represented by the vertical lines. Picture: CWI

CWI researcher Tomas Klos modelled chances of reliability, based on Bayes' Rule. These chances can be depicted in a figure. When nothing is known, the chance distribution starts as a horizontal line: a neutral reputation. After several events it begins to look like a mountain shifting to one side: A peak on the right indicates that an agent is almost always reliable, whereas a peak on the left indicates that it is not to be trusted. Klos and others also developed an international test-bed with annual competitions, to realize an environment where researchers can objectively compare the results of their individual software agents. The SEN4 results will be used in a scheduled pilot project with Falck security.

Future

Now the research results and concepts are being used in Almende's ASK system, but will it ever be used for emergencies? To test it in a more neutral and less stressful environment, the system was set up at an employment agency. Fifty freelancers received e-mails or SMS messages asking if they could work at a certain time. Without knowing that they were only talking to a computer, they all typed in the answer. Where it took one person at the employment agency 8 hours to call and schedule 50 people, the ASK system performed the same task in less than three minutes. The CIM team hopes that these kinds of successes help to win confidence and create the opportunity to test the system within both simulated and real emergency situations. It is all about coping well with small risk situations that can have big consequences.

The CIM project started in 2003 and is being financed by SenterNovem. CWI's research partners in this project are the Technische Universiteit Delft, the Vrije Universiteit Amsterdam, Almende, CMotions and Falck.

MonetDB/XQuery: Searching XML databases in record time

Fast and efficient data management is a key factor in IT. Ever more data is being stored in XML format, which can be searched through with the XQuery language. Computer scientists of CWI, the University of Twente and the Technische Universität München launched the high-performance MonetDB/XQuery system on 1 June 2005. This open source system searches large XML databases in record time.

Traditionally, companies used to store business information like addresses and prices in tables with strict relationships between rows and columns. Although the table format is suitable for regularly structured data, it cannot handle unstructured data. Nowadays, enterprises increasingly store their information in XML – the Extensible Markup Language, designed by the World Wide Web Consortium (W3C). This de-facto standard is very flexible because of its ability to describe and manipulate many different kinds of data, like memos, log files, and web pages. XML data can easily be shared between various organizations. In the IT industry, XML is often used as data format for exchanging information in Service Oriented Architectures (SOA) and integrating data from multiple sources in Enterprise Application Integration (EAI) systems.

Could the efficiency of XML databases be made comparable to those of traditional relational databases? This was not obvious from the start. Relational database systems using the SQL query language are able to search large amounts of data efficiently. This is due to the well-defined database structure, automatic query optimization, and the use of index structures. For the great variety of XML texts this is more difficult. The XQuery language is specifically designed to pose queries over data with little or irregular structure, but not necessarily efficiently. Building a database system that can do this was a big challenge, which could only be met by advancing database query processing, optimization and indexing. In the past decade, much research at academic institutes and in industry labs was being spent on this subject. CWI, the Technische Universität München and the University of Twente released an XML database system – MonetDB/XQuery – that broke all speed records for complex queries on large databases.

Innovative technology

The idea behind MonetDB/XQuery is to re-use mature relational database technology for XML. To make this possible, researchers at CWI use an 'isomorph' (lossless, two-way) mapping between XML documents and relational tables – see the information box. This has many advantages, for instance in speed. Previous XQuery systems all handled for-loops with one-at-a-time evaluation strategies that respected the iteration order. MonetDB/XQuery can abstract from the sequential order. This allows the use of faster relational query processing algorithms and it enables better query optimization by performing query steps in a different order.
CWI computer scientists Peter Boncz and Stefan Manegold further invented a number of new algorithms for the processing of 'join'-queries. It turns out that performance can be won if the database system is aware that tables representing XML do not contain random numbers (see second information box), due to the specific tree structure of XML. This advantage is exploited fully by the 'loop-lifted staircase join' family of algorithms that provide the core functionality in XML querying. New releases of MonetDB/XQuery have followed since.

MonetDB/XQuery was extensively benchmarked and compared with other XML database systems. It is generally acknowledged to be the fastest system when complex join-queries or large documents are involved. The heart of the system is formed by the high-performance MonetDB database kernel, of which Peter Boncz studied the design in his PhD dissertation. MonetDB also was the processing engine behind the succesful CWI data mining spin-off company DataDistilleries, which was acquired by SPSS Inc. in 2002.

Forensic research

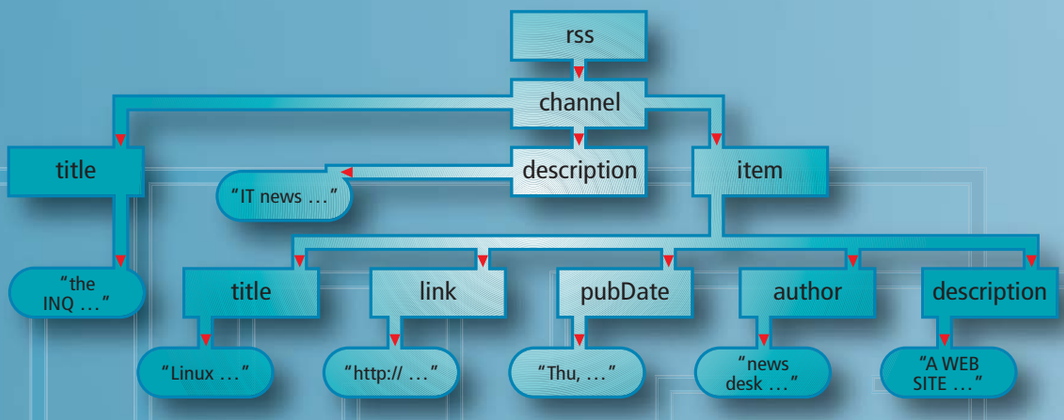
Various organizations are using the new open source system, and the 'Database Architectures and Information Access (INS1) research group of CWI is collaborating with a number of partners. One of those is the Netherlands Forensic Institute (NFI). This institute investigates hardware taken into custody, like mobile phones and harddisks, to recover e-mails or to know "which information was written on the evening of the 21st of April". Together with CWI, NFI has built an integrated forensic workbench that integrates a wide variety of forensic search tools. After producing XML data NFI researchers use the Xquery language to query it. Performance is very important as the number of investigated PCs

A brief intro in XML databases

XML: What does it look like and how is it queried? Take, for example, an arbitrary RSS news feed from www.theinquirer.net/inquirer.rss [1]:

```
<rss version="0.91">
  <channel>
    <title>the INQUIRER</title>
    <description>IT news - never knowingly undersoldered</description>
    <item>
      <title>Linux OS "just as bloated as Windows"</title>
      <link>http://www.theinquirer.net/default.aspx?article=33601</link>
      <pubDate>Thu, 10 Aug 2006 14:15:11 GMT</pubDate>
      <author>newsdesk@theinquirer.net</author>
      <description>A WEB SITE has launched into an attack on the 15 year old Linux in
a tirade which puts the attack on James I in the shade.</description>
    </item>
</channel>
</rss>
```

XML information consists of element-nodes between brackets, like <rss>. These are comparable to tags in HTML. Enclosed between such tags text-nodes can be found. The resulting structure can be seen as a tree. In the above example, the <rss> element is the root, with a single <channel> element-node in it. This element-node has three children: <title>, <description> and <item>. Text is stored in separate text-nodes.



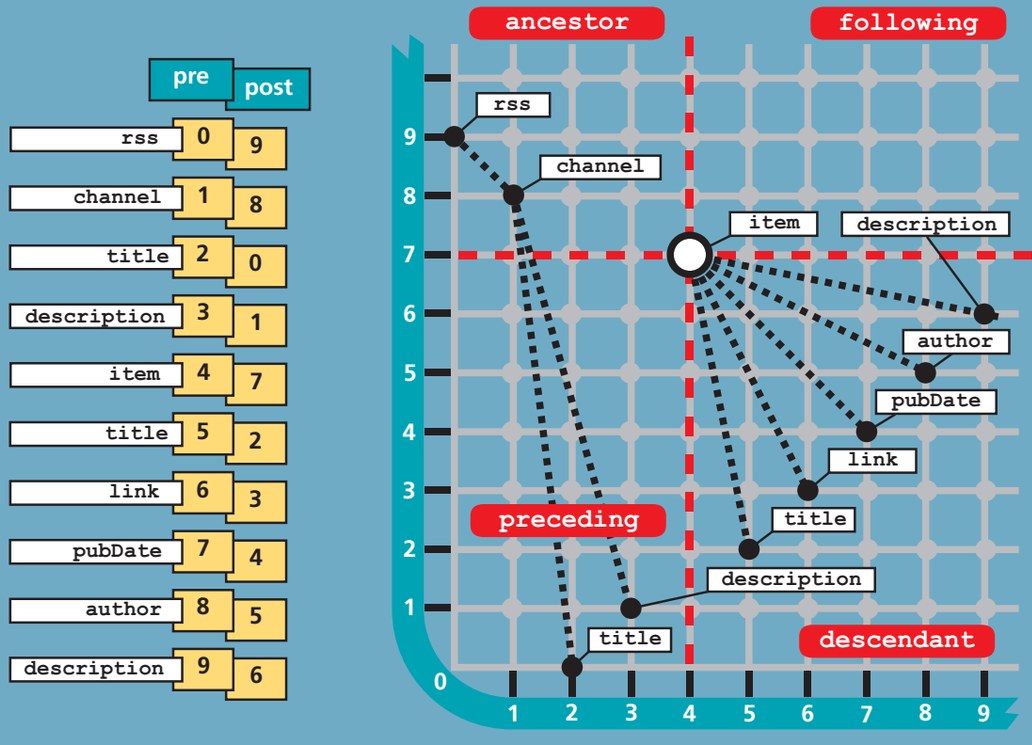
What about queries? In XML, the XQuery language plays the role that SQL does for relational database. It can handle queries like: "Find all products that are red in the category MP3 player and for all of these products, give the list of sellers, the prices and addresses" but also more complex ones. Whereas in the SQL queries follow the 'SELECT..FROM.. WHERE' pattern, XQuery statements follow a 'For-Let-Where-Return' pattern (FLWR – pronounced "Flower"). In the following example XQuery asks for all headlines about Linux from the IT news site The Inquirer:

```
for $item in doc('http://www.theinquirer.net/inquirer.rss')/descendant::item
let $title = $item/child::title
where contains($title, 'Linux')
return $item
```

[1] CWI is not responsible for the content

Storing XML in relational databases

XML can be translated into a relational database format. Two numbers, 'pre' and 'post' are assigned to each node in the tree. The pre-numbers follow the order of opening of tags, the post-numbers the order of closing them. The yellow table below fully represents the XML tree from the first information box. When pre and post are viewed as the (X, Y) coordinates of a two-dimensional plane, the merits of this representation become clear: The four quadrants of the plane correspond to the four database relationships ancestor, descendant, preceding and following. These are crucial components in the XQuery language. Thus, we can map an XQuery 'tree-query' that asks for all descendants of `<item>` (pre=4, post=7) to the SQL 'table-query': `SELECT * FROM table WHERE pre>4 and post<7`. This method is being used by the MonetDB/XQuery system.



can amount to hundreds, for instance in fraud cases. NFI found MonetDB/XQuery the only system meeting their requirements in terms of performance and scalability.

Future research

In 2006, W3C is expected to come with a first proposal for an XQuery Update Facility that will allow changing the contents of XML databases. CWI works on a version of MonetDB/XQuery that supports this. As such, XML transaction magement provides a number of open challenges for which additional research is needed. Since XML information is less structured than relational data, XML information retrieval like keyword search is expected to be mixed into query processing. Finally, since XML is pervasive on the web, a research project in the area of distributed XML databases is underway. For this purpose MonetDB/XQuery is being extended with distributed query execution, P2P data structures and P2P data dissemination methods. These three research projects will be pursued at CWI in cooperation with the University of Twente in the context of the MultimediaN Bsik project.

More information: http://monetdb.cwi.nl

Niet
met water
blussen
NIETS VOORPLAATSEN

Safety measures for future cyber security

Credit card information, classified e-mails or confidential enterprise details: For cyber communications it has always been important to be at least one step ahead of the capacities of malicious hackers and other criminals. To provide sufficient protection, scientists are working on the basic concepts for future security. The Cryptology and Information Security research group at CWI explores and develops the latest theories, including quantum cryptography, secure computation and public-key cryptography.

Until recently, digital security was mainly concerned with providing authenticity and security of communication in the presence of hackers. This was done by cryptographic methods like encryptions, which are based on the assumption that some computational problems are difficult to solve. RSA encoding is, for example, based on the difficulty of factoring large integers into prime numbers. In 1999, CWI scientists coordinated the factorization or 'cracking' of the RSA-512 code, which was then commonly used for internet security. It was indeed rather difficult: It took seven calendar months, 300 computers and one supercomputer to factorize the number of 512 bits (155 digits). As a result, today's implementations are based on much larger numbers.

Nowadays, even more complex security issues can be tackled by using new cryptographic techniques. Consider, for example, negotiations between several parties who do not trust each other, like two enterprises negotiating a fusion. One thing they would like to know is if their customer database will grow considerably after joining or, on the contrary, will show much overlap between their clients. They do not want to share the actual data, in case their potential fusion partner will misuse these for their own marketing. This is an example of 'Secure Cooperation'. Methods like RSA cannot provide security for cooperation between mutually distrusting parties. This problem needs other methods to tackle its complexity.

Serge Fehr, researcher at CWI, investigates a new Secure Cooperation technique, using quantum cryptography – information security by applying quantum mechanics. This might be applied to high and medium security issues, like protection of access control to nuclear weapons or identification for cash points. For this work, he received a Veni subsidy from the Netherlands Organisation for Scientific Research (NWO) on 20 December. In order to obtain security Fehr studies the Bounded-Quantum-Storage Model, which exploits the technological difficulty of storing photons without disturbing their quantum state. The basic idea is to swamp potential adversaries with more quantum information than they can possibly store. Advantages are great: Adversaries may be arbitrarily powerful, and in particular they may have unbounded computing power. Swamping the adversary's quantum memory requires very little, since with today's technology storing quantum states in a reliable way is essentially impossible.

According to Heisenberg's Uncertainty Principle (well-known in quantum physics), converting quantum information to classical information by measuring it destroys some of that information in an irreversible way. The challenge is to design schemes where the adversary cannot afford this loss while honest users can, and to come up with rigorous mathematical security proofs showing that if the adversary fails to store enough quantum information he can indeed not obtain classified information or provoke a malfunction.

The main disadvantage of this approach is that non-standard communication devices need to be employed that allow for quantum communication. These devices can for example use the polarisation of light. (A quantum computer is not necessary.) A particularly interesting advantage of the Bounded-Storage Model is 'everlasting security': If the adversary fails to store crucial quantum information during the execution of the scheme, then his chance of breaking it is lost forever, no matter how powerful he will be in the future. This is in sharp contrast to conventional computational cryptography, in which schemes may be broken afterwards once an adversary has gained sufficient computing power.

Secure computation breakthrough

Apart from quantum cryptography, CWI focuses on many other aspects of cryptology. Ronald Cramer, head of the Cryptology and Information Security (PNA5) group, has discovered promising connections between algebraic number theory, algebraic geometry and the problem of securely simulating a 'trusted third party'. If people or organizations do not trust each other, it would be convenient to have a neutral third party that honestly performs the computations whilst keeping the content secret. However, in many scenarios the-

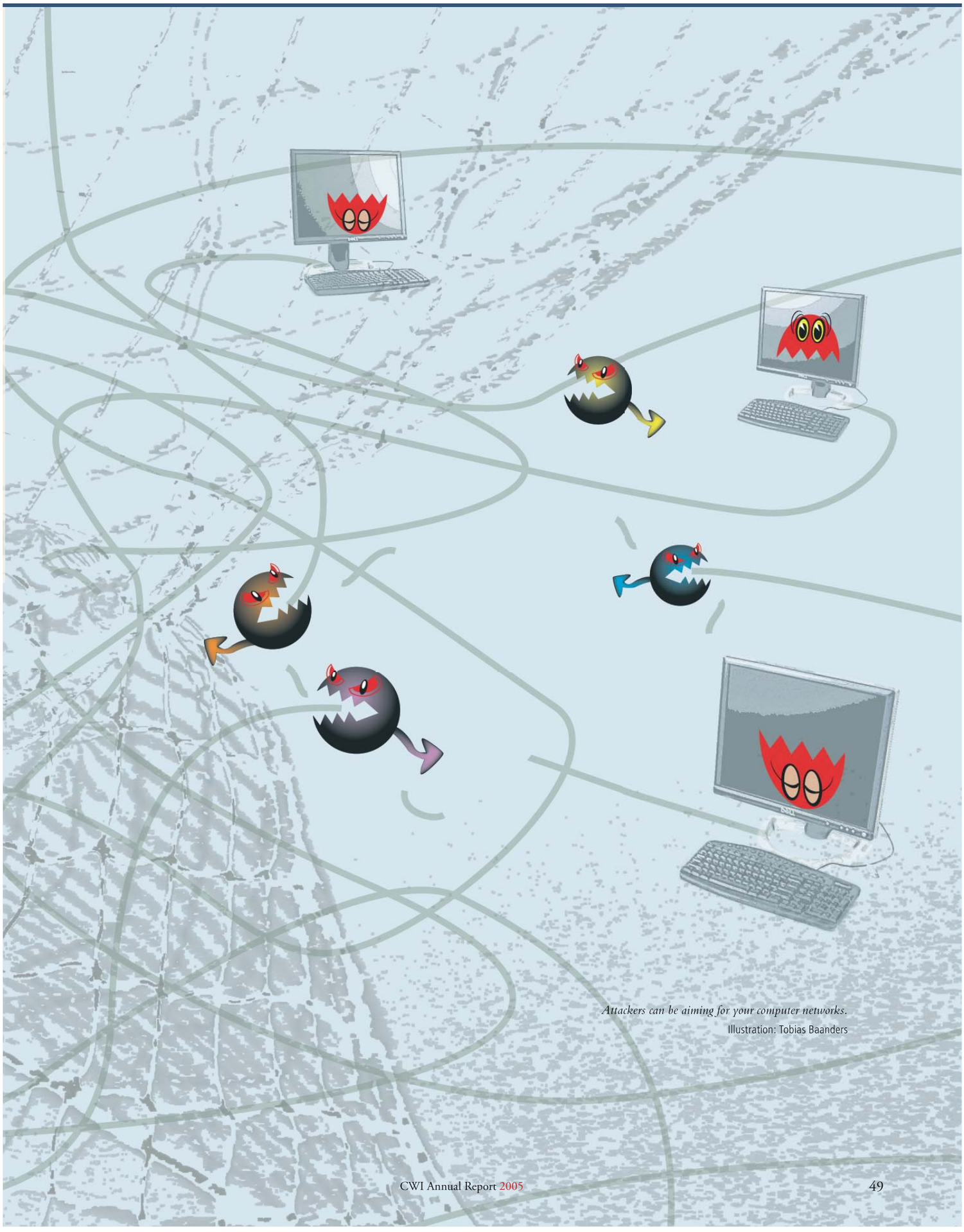
re is no such party. Cryptographic techniques can simulate this virtual party by means of carefully designed interactive protocols. As long as a majority of the involved processors are honest, such simulations are secure in a way that they are as good as a real trusted party.

Technically, a trusted-player simulation – also called multiparty computation – is usually done as follows. Each processor in a network has a private input, and the purpose is to evaluate a given function on these inputs without revealing those inputs. To this end, each private input is split up into parts that do not reveal anything about the secret input data by using a method called secret sharing. With dedicated techniques the network can securely generate secret sharings of additions and multiplications of already secret-shared values. Finally the resulting parts are combined in order to reveal the legitimate outcome and nothing but the legitimate outcome (for example '11% of the customer databases overlap'). Using sophisticated techniques from algebraic geometry, in particular results about algebraic curves with many rational points, Ronald Cramer recently developed new methods for secret sharing and secure computation that can be more efficient than existing ones.

Besides the described techniques, the Cryptology and Information Security research group at CWI focuses on all aspects of cryptology, such as computational number theory, information-theory-based cryptography, public-key cryptography, cryptographic protocols, and formal security analysis. Fundamental research of cryptography at this group can influence the practical feasibility of security technology and can be of significance for computer security, financial transactions via internet and even national security.

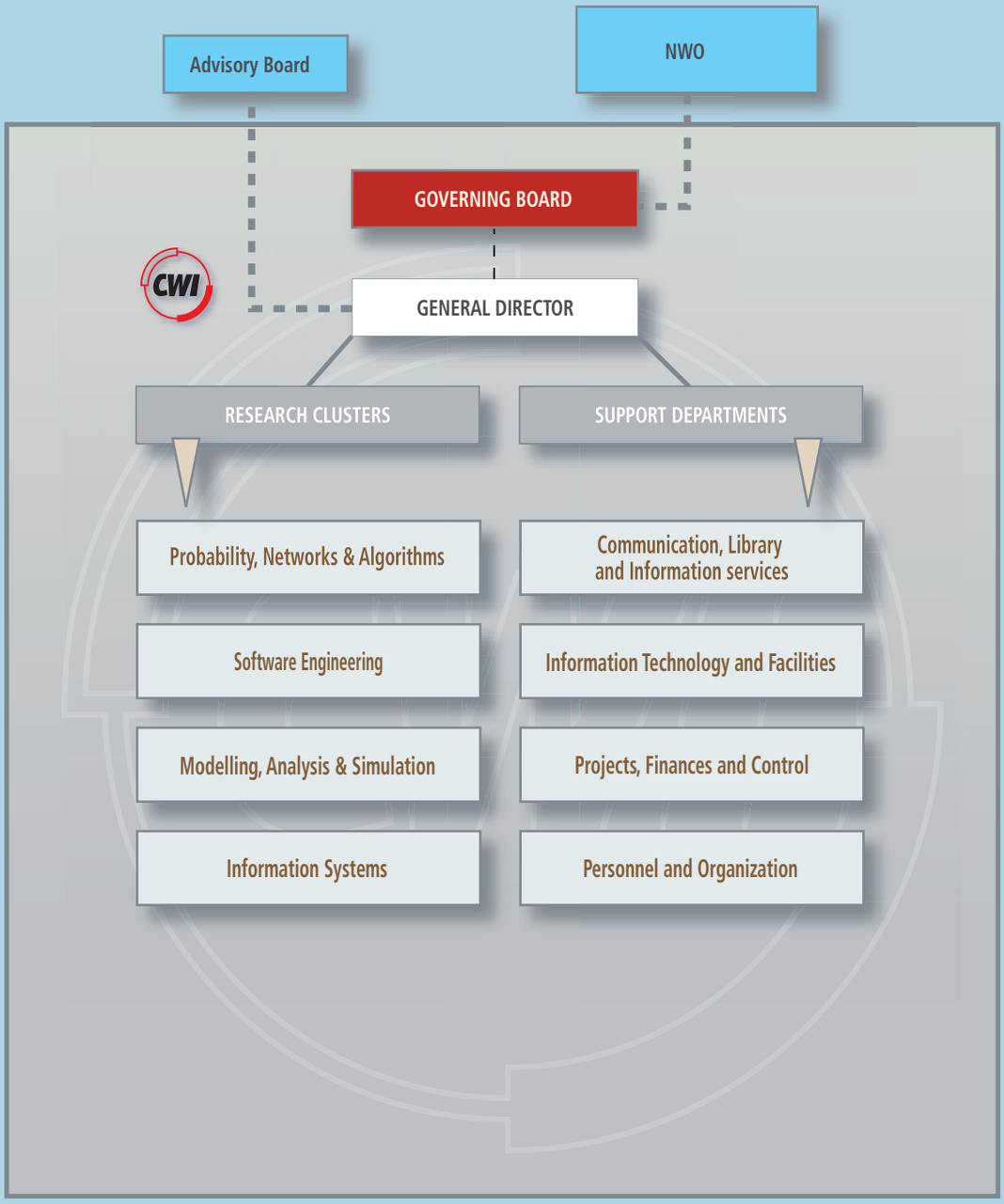
Serge Fehr

Ronald Cramer



Attackers can be aiming for your computer networks.
Illustration: Tobias Baanders

Appendices


Advisory Board
NWO
GOVERNING BOARD
CWI
GENERAL DIRECTOR
RESEARCH CLUSTERS
SUPPORT DEPARTMENTS
Probability, Networks & Algorithms
Communication, Library and Information services
Software Engineering
Information Technology and Facilities
Modelling, Analysis & Simulation
Projects, Finances and Control
Information Systems
Personnel and Organization

Organization

Research

Cluster Theme	Cluster leader Theme leader
Probability, Networks and Algorithms	**A.M.H. Gerards**
Algorithms, Combinatorics and Optimization (formerly: Networks and Logic – Optimization and Programming)	M. Laurent
Performance Analysis of Communication Networks (formerly: Advanced Communication Networks)	M.R.H. Mandjes
Stochastic Dynamics and Discrete Probability (formerly: Stochastics)	J. van den Berg
Signals and Images	E.J.E.M. Pauwels
Cryptology and Information Security	R.J.F. Cramer
Software Engineering	**P. Klint**
Interactive Software Development and Renovation	P. Klint
Specification and Analysis of Embedded Systems	J.C. van de Pol
Coordination Languages	J.J.M.M. Rutten
Computational Intelligence and Multi-agent Games (formerly: Evolutionary Systems and Applied Algorithmics)	J.A. La Poutré
Distributed Multimedia Languages and Infrastructures (formerly: Convergent Media Infrastructures)	D.C.A. Bulterman
Modelling, Analysis and Simulation	**J.G. Verwer**
Nonlinear PDEs: Analysis and Scientific Computing	A. Doelman
Computing and Control	B. Koren
Nonlinear Dynamics and Complex Systems	U. Ebert
Information Systems	**M.L. Kersten**
Standardization and Knowledge Transfer	M.L. Kersten
Database Architectures and Information Access	M.L. Kersten
Semantic Media Interfaces (formerly: Multimedia and Human-Computer Interaction)	L. Hardman
Visualization and 3D Interfaces	R. van Liere
Quantum Computing and Advanced Systems Research	H.M. Buhrman

Management

Management Team

J.K. Lenstra (general director)
M.L. Kersten
P. Klint
A. Schrijver, until 1 June
A.M.H. Gerards, from 1 June
J.G. Verwer (cluster leaders)
D.G.C. Broekhuis (controller)

Governing Board

P.W. Adriaans (Universiteit van Amsterdam), chairman
C.J. van Duijn (Technische Universiteit Eindhoven)
F.A. van der Duyn Schouten (Tilburg University)
J.N. Kok (Universiteit Leiden), from 1 July
M.H. Overmars (Utrecht University), until 1 July
S.J.M. Roelofs (Nederland~ICT)

Support

Communication, Library and Information services (CBI)

(formerly: Communication & Publication Department – G.M.T. Nieuwendijk, and Library & Information Services - A.L. Ong)
G.M.T. Nieuwendijk

Information Technology and Facilities

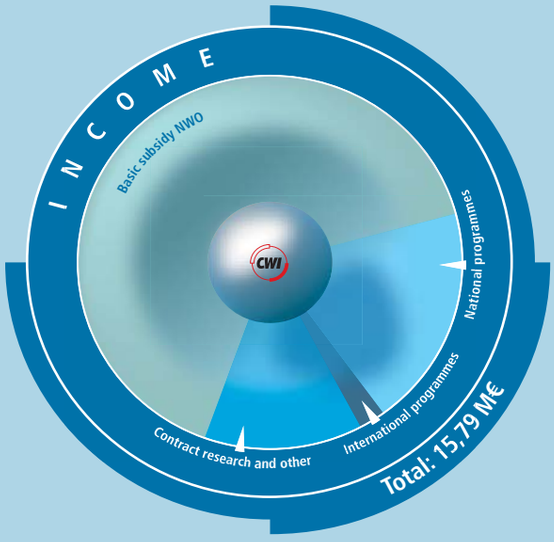
(formerly: Computer Systems & Telematics – I.L. Dijkstra, and Facility Department-F.J.G. Goudsbloem)
I.L. Dijkstra

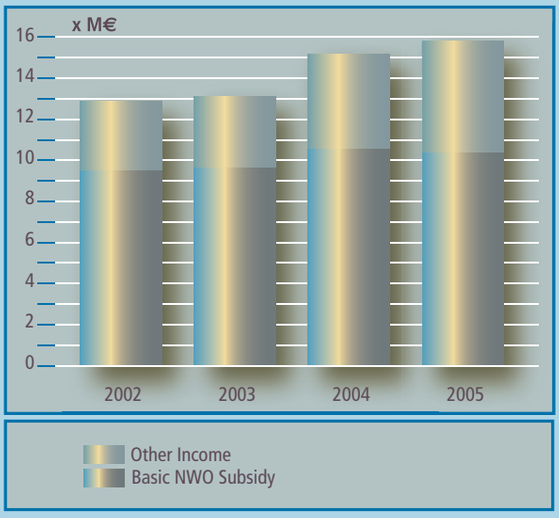
Projects, Finances and Control

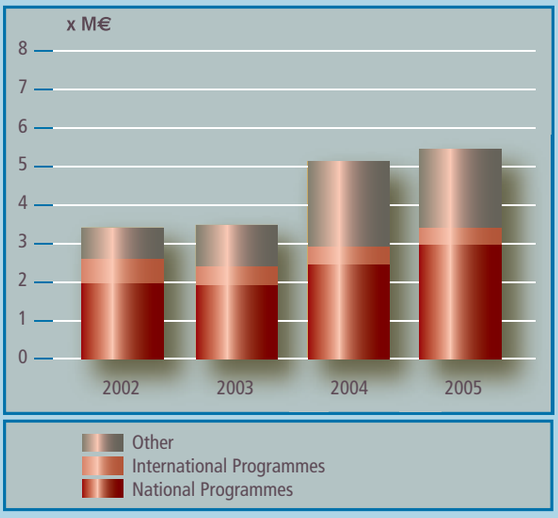
(formerly: Financial Department - E. de Boer)
D.G.C. Broekhuis

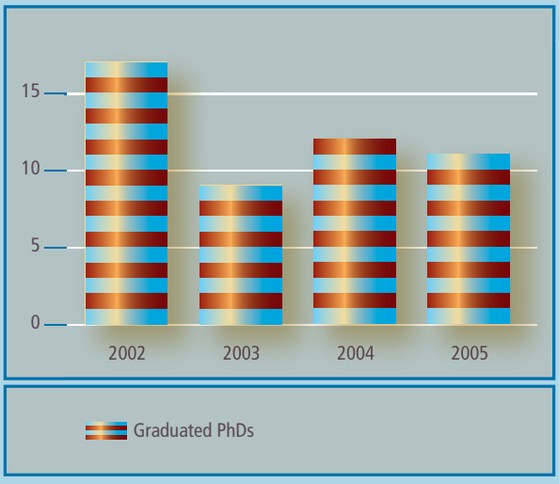
Personnel and Organization

(formerly: Personnel Department)
J. Koster

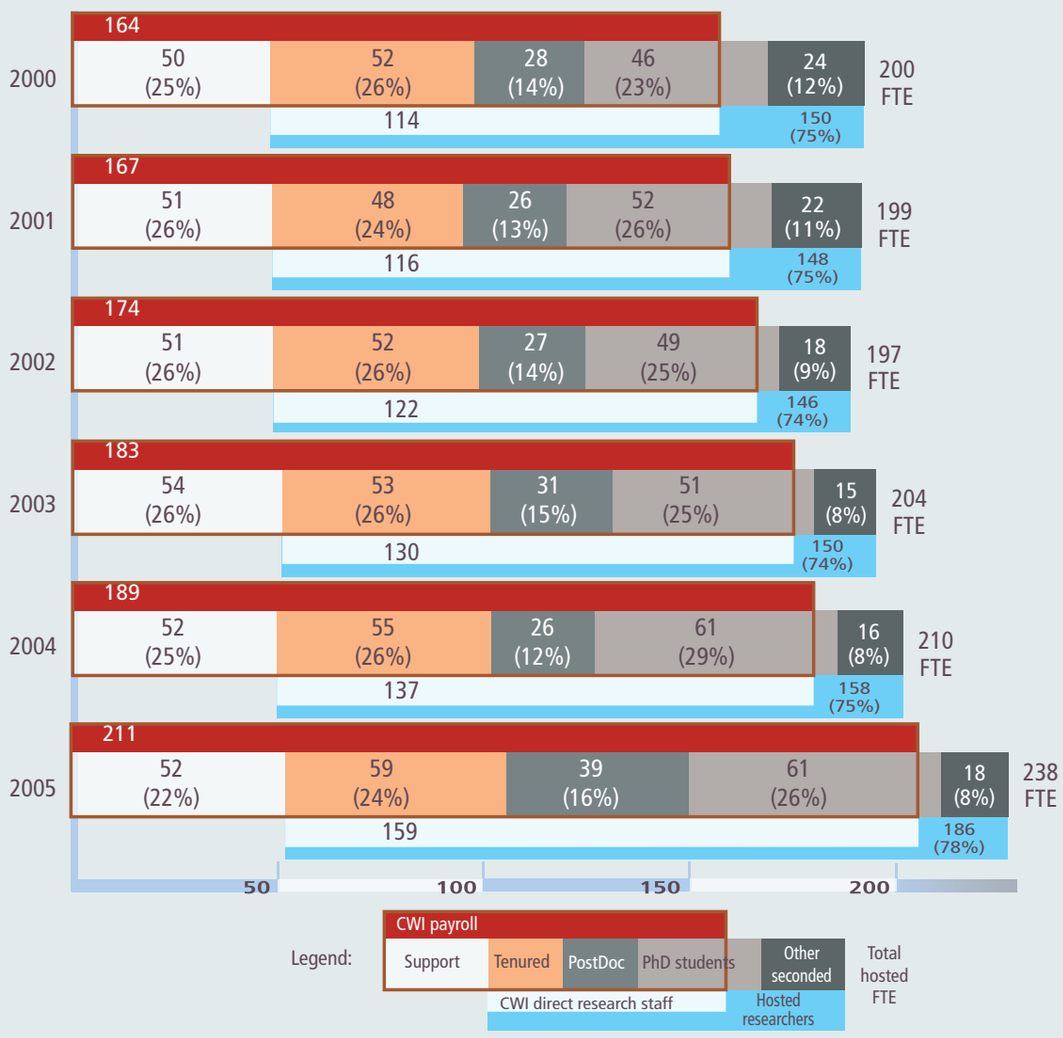

INCOME
Basic subsidy NWO
National programmes
International programmes
Contract research and other
Total: 15,79 M€


x M€
16
14
12
10
8
6
4
2
0
2002
2003
2004
2005
Other Income
Basic NWO Subsidy


x M€
8
7
6
5
4
3
2
1
0
2002
2003
2004
2005
Other
International Programmes
National Programmes


15
10
5
0
2002
2003
2004
2005
Graduated PhDs

CWI staff 2000-2005



Statistics of CWI output 2002-2005

	CWI				PNA				SEN				MAS				INS			
	2002	2003	2004	2005	2002	2003	2004	2005	2002	2003	2004	2005	2002	2003	2004	2005	2002	2003	2004	2005
Refereed journals or proceedings	260	316	308	391	60	105	62	99	79	89	131	173	58	54	74	49	63	68	41	70
Other journals or proceedings	28	27	22	37	10	7	8	4	10	14	5	10	2	1	2	6	6	5	7	17
Monographs	9	6	5	5	1	2	2	3	4	0	3	2	1	1	0	0	3	3	1	0
Book chapters	12	10	14	10	4	3	9	5	4	3	2	3	0	0	1	0	4	4	2	2
PhD Theses	17	9	12	11	2	2	1	4	7	3	6	4	4	3	3	3	4	1	2	0
Professional products and other output	116	138	94	131	33	51	31	50	32	39	38	38	9	9	12	15	42	39	13	28
Total	442	506	455	585	110	170	113	165	136	148	185	230	74	68	92	73	122	120	66	117

CWI 2005 staff numbers

Male/female staff in FTE at the end of 2004 (CWI payroll)

	Research	Support
Male	138.1	32.3
Female	21.3	18.7

Master students in numbers

2002	2003	2004	2005
13	16	21	16

International staff in 2005 in FTE/year

Australia	1.0	Iran	1.0
Austria	1.0	Israel	1.0
Belgium	3.8	Italy	3.0
Bosnie-Herzegovina	1.0	Moldavia	1.0
Bulgaria	2.0	Poland	4.0
China	2.0	Rumania	2.0
Czech Republic	3.0	Russia	4.0
France	3.8	Spain	4.5
Germany	10.8	Switzerland	1.0
Great Britain	6.0	Turkmenistan	1.0
Greece	2.0	Ukraine	0.7
Hungary	1.0	USA	4.5
Indonesia	1.0	Vietnam	1.0

Total non-Dutch in FTE 67 (42%)
Total CWI research staff in FTE 159

International staff at CWI in numbers 2002-2005

Year	# Persons	# Nationalities	# European nationalities
2002	63	25	17
2003	76	25	16
2004	75	26	18
2005	69	26	18

Research Clusters and themes

Probability, Networks and Algorithms

Cluster leader: A.M.H. Gerards

Algorithms, Combinatorics and Optimization

Formerly: Networks and Logic – Optimization and Programming

Theme leader:
M. Laurent

The design, analysis and implementation of optimization and approximation algorithms for combinatorial problems arising, in particular, from combinatorial optimization, game theory, molecular biology, mobile networks, production and transportation planning, scheduling, time-tabling. The methods come from mathematics (graph theory, discrete mathematics, topology, algebra, geometry), operations research (integer, linear, semidefinite and constraint programming), and computer science (complexity theory).

Combinatorics and Optimization: Investigation of combinatorial, geometric and algebraic methods in combinatorics and optimization.

Constraint and Integer Programming: Foundations and the applications of integer and constraint programming, including their cross-fertilization and links to game theory.

Algorithmic and Combinatorial Methods for Molecular Biology: The mathematical analysis of molecular structures in biology and the design, analysis and implementation of algorithms for computational molecular biology.

Performance Analysis of Communication Networks

Formerly: Advanced Communication Networks

Theme leader:
M.R.H. Mandjes

Traffic Modelling, Analysis, and Performance: Development of queueing-theoretic models and methods to study congestion phenomena in communication networks under new traffic paradigms. Focus is on the impact of heavy-tailed file size distributions and self-similar traffic patterns.

Wireless Networks: Development of analysis techniques for dimensioning, engineering, and operating wireless networks. Special attention is devoted to capacity gains from user mobility and opportunistic scheduling algorithms in wireless data transmission.

Service Differentiation: Investigation of fundamental research issues raised by quality of service differentiation in wired and wireless communications. A central role is played by the integration of streaming (voice, video) and elastic (file transfer, web browsing) services.

Performance of Distributed ICT Systems: Development and analysis of quantitative models for predicting and controlling the end-to-end quality of service in next-generation large-scale distributed ICT infrastructures, explicitly taking into account the combined impact of information systems and communication networks.

Stochastic Dynamics and Discrete Probability

Formerly: Stochastics

Theme leader:
J. van den Berg

The mission of this theme is theoretical and applied research at the frontiers of modern probability, in particular on problems motivated by biology, (geo-) physics, finance and technology. The theme consists of two subthemes, Probability and Stochastic Analysis.
Probability: Research on stochastic systems with a large number of interacting components; these are motivated by a variety of biological and physical processes and by problems concerning wireless communication networks.
Stochastic Analysis: Fundamental and applied research, in particular spectral analysis of Gaussian processes and fields based on the theory of vibrating strings, with special interest to stochastic models in mathematical finance and queueing systems driven by scalar or spatial fractional Brownian motions.

Signals and Images

Theme leader:
E.J.E.M. Pauwels

Image Understanding, Retrieval and Indexing investigates mathematical methodologies to generate content-specific descriptions of images and video, for the purpose of robust indexing, understanding and retrieval from large databases.
Image Representation and Analysis deals with multi-resolution signal and image representations in general and methods in wavelet analysis and mathematical morphology in particular. Furthermore, it seeks to use such representations for problems in image analysis and coding. This group has recently branched out into biometrics.
Stochastic Geometry is concerned with the modelling and analysis of random geometric structures using techniques from spatial statistics and stochastic geometry.

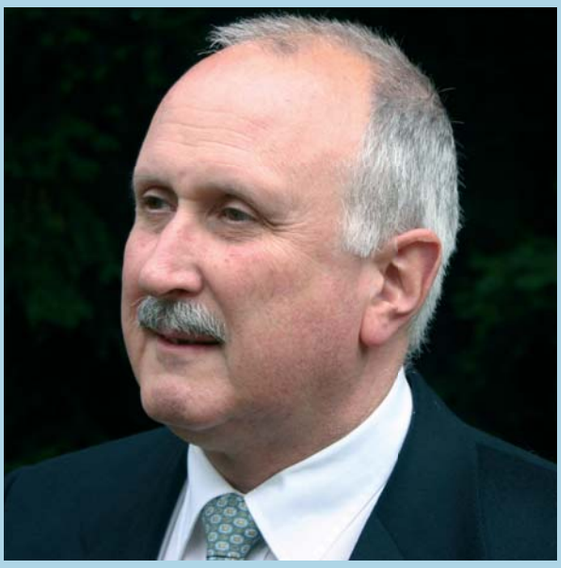
Cryptology and Information Security

Theme leader:
R.J.F. Cramer

Mathematical cryptology: problems reducible to standard (computational) mathematics, algebraic geometric/number theoretical secure computation and secret sharing, cryptanalysis (Number Field Sieve (NFS) for factoring RSA-moduli, algebraic cryptanalysis), algebraic complexity.
Highly composed security systems: models, universal composability, simulatability, interaction with formal methods, theoretical cryptography.
Public-key cryptography: chosen ciphertext security, signatures, identity-based encryption, dedicated secure multi-party protocols.
Quantum cryptography and information theory: quantum oblivious transfer, privacy amplification, alternative (non-complexity-theoretic) security enablers (quantum bounded storage).
Computational Number Theory and Discrete tomography: algorithmic number theory (NFS, computational issues concerning Riemann hypothesis), algorithmic reconstruction of objects from projections.

Software Engineering

Cluster leader: P. Klint



Interactive Software Development and Renovation

Theme leader:
P. Klint

Software Evolution: Development of methods, tools, and techniques that help to make and keep software systems sufficiently flexible.
Software Transformation: Improvement of run-time efficiency (optimization), improvement of static structure (refactoring), and systematic modification (computer-aided maintenance) of software systems.
Generic Language Technology: Increased applicability and usability of our generic language technology as embodied in the ASF+SDF Meta-Environment is achieved by the steady introduction of new technologies like lexical matching and rewriting, generic pretty printing, information visualization and user-interface extensibility. The introduction of a relation calculator has created new perspectives on fact extraction from source code and on source code analysis.
Concept-Based Reasoning and Knowledge Engineering: Applied logic research covering a broad spectrum of aspects, like dynamic logic, tableau reasoning, construction of electronic textbooks for logic, and interactive information engineering.

Specification and Analysis of Embedded Systems

Theme leader:
J.C. van de Pol

This group studies modelling and validation techniques for computer controlled systems, which allow more efficient designs and constructions with fewer embedded faults. This is achieved by developing and implementing algorithms for the analysis and verification of distributed systems. The current focus is on symbolic model transformations, and on parallel algorithms for model checking.
The group applies new techniques for theorem proving, testing and (distributed) model checking with industrial partners to various case studies, for instance, communication protocols, embedded controllers, software architectures, safety-critical railway interlockings, and security protocols for e-commerce. The purpose is to establish the correctness of programmed systems 'beyond reasonable doubt'.

Coordination Languages

Theme leader:
J.J.M.M. Rutten

The activity in SEN3 ranges from mathematical models of behaviour and computation to experimental systems and demonstrator applications. SEN3 aims to provide the technology for coordination and dynamic composition of concurrent systems, based on solid mathematical foundations. Systems of special interest include long-lasting distributed applications, component-based systems, and service-oriented computing. Building such concurrent systems by composition of

independent components and services involves coordination of their mutual interactions. Coordination, for instance, through connector circuits, is therefore one of the central subjects of the research in this group.

Computational Intelligence and Multi-Agent Games

Formerly: Evolutionary Systems and Applied Algorithmics

Theme leader:
J.A. La Poutré

This research group focuses on the combination of (distributed) adaptive computation with application-oriented fields of economics, management, health-care, and e-societies, like for e-commerce. Typical applications concern markets and market mechanisms, negotiation, auctions, and social aspects. The concept of agents in computer science, economics and social sciences yield important areas of research. In these cases, adaptive behaviour of agents, based on their own point of view ('bounded rationality') in a dynamic environment is essential. To allow learning in distributed systems of interacting agents, machine learning techniques like evolutionary systems, neural networks and adaptive algorithms are investigated. These algorithms then form the 'heart' of learning agents in application systems and simulated markets. Insights gained from these activities apply to agent technology – how to build truly learning agents and agent systems – as well as, e.g., economics – how to simulate adaptive agents.

Distributed Multimedia Languages and Infrastructures

Formerly the pilot theme: Convergent Media Infrastructures

Theme leader:
D.C.A. Bulterman

The goal of this research group is to study methods for the specification, scheduling, and verification of composite presentations that are distributed heterogeneous collections of underlying devices and networks based on an abstracted homogeneous environment. The research studies desktop, consumer electronics and mobile delivery platforms and include the development of languages, user models and experimental implementation platforms based on the Ambulant Player.

Modelling, Analysis and Simulation

Cluster leader: J.G. Verwer

Nonlinear PDEs: Analysis and Scientific Computing

Theme leader:
A. Doelman

Scientific Computing in the Life Sciences: Mathematical modelling, mathematical and numerical analysis, and numerical simulation for life sciences, in particular biology and medicine. Cooperation has been established with researchers working in cell, neuro, and microbiology.
Nonlinear Dynamics of Natural Systems: Mathematical analysis of finite and infinite dynamical systems in interaction with the earth and life sciences. This research is embedded in the national mathematics cluster Nonlinear Dynamics of Natural Systems (NDNS).
Geometric Integration of Wave Phenomena: Numerical analysis and simulation of partial differential equations, in particular structure-preserving numerical methods with applications to conservative continua like geophysical fluids.
Asymptotics and Special Functions: Research on uniform asymptotic expansions and numerical and algebraic algorithms for special functions.

Computing and Control

Theme leader:
B. Koren

Computational Fluid Dynamics and Computational Electromagnetics: Current research focuses on efficient solution methods for steady, two-fluid Navier-Stokes flows, immersed boundary methods for Navier-Stokes flows around complex geometries, shape-optimization methods for electromechanical devices, stochastic methods for electromagnetic field computations, and parallelization of software for fluid-structure interaction.
Control and System Theory: Research on problems of control and system theory for various dynamic systems motivated by control problems of engineering and by cell biology. Current research is directed at control of hybrid systems, realization theory for subclasses of hybrid systems, supervisory control of decentralized and modular discrete-event systems, and computational properties of nonlinear systems.

Nonlinear Dynamics and Complex Systems

Theme leader:
U. Ebert

This theme focuses on nonlinear dynamics and model reduction, presently mainly applied to spark formation in technology and geophysics – a challenging problem on multiple scales. On the level of partial differential equations,

the group concentrates on numerical questions of operator splitting, monotonicity preservation and adaptive grid refinement. The group further focuses on analytical front dynamics, reduction to free boundary problems and solutions with conformal mapping methods. Model reduction on a different level takes place when partial differential equations are coupled to stochastic models in so-called hybrid models. The theme leader holds a part-time professorship in physics in Eindhoven where she plans and interprets spark experiments in the range of her theoretical research.

Information Systems

Cluster leader: M.L. Kersten

Standardization and Knowledge Transfer

Theme leader:
M.L. Kersten

Knowledge transfer on evolving standards, primarily within the context of the World Wide Web Consortium (W3C). This includes general management of all W3C offices worldwide, leadership of the W3C HTML Working Group, co-leadership on the W3C XForms activities, and participation in the work of the Document Format domain of W3C.

Database Architectures and Information Access

Theme leader:
M.L. Kersten

Multimedia Databases: Development of an efficient storage and retrieval system of multimedia data. The research line on multimedia information retrieval aims at developing a multimedia database system, which can offer a high level of abstraction to both developers of end-user applications and researchers working on content analysis techniques.
Database Architectures: Development of the next generation database technology to support Ambient Intelligence applications. Ambient Intelligence refers to digital environments in which multimedia services are sensitive to people's needs, personalized to their requirements, anticipatory of their behaviour and responsive to their presence.
Query Languages & Optimization: Development of a multi-layer query optimizer infrastructure to support multimedia information access. At the core of such a system we envision a sound and flexible probabilistic model to steer the retrie-

val process, integrated with query optimizers and kernel functionality.
MonetDB Dissemination: Promoting the development and use of the database experimentation platform MonetDB. MonetDB is an open source high-performance database system developed at CWI, designed to provide high performance on complex queries against large databases, e.g., combining tables with hundreds of columns and multi-million rows.

Semantic Media Interfaces

Formerly: Multimedia and Human-Computer Interaction

Theme leader:
L. Hardman

Investigation of the boundaries between multimedia and the Semantic Web and development of models and tools for automatic generation of high-quality hypermedia presentations, taking into account design knowledge, user characteristics, and platform-specific requirements. This includes the modelling of argument structures for the generation of meaningful video sequences, domain-independent structuring of a semantically annotated media repository for presentation to end-users, dependencies of the user and domain models in the generation process, characteristics of media types for presenting information to the user, and to what extent graphic design knowledge can be included in the generation process.

Visualization and 3D Interfaces

Theme leader:
R. van Liere

Data Visualization: Projects in the application area of the Dutch Living Cell initiative. Key research focus is the interactive visualization of time dependent data sets and the exploration of multidimensional information spaces. Furthermore, the problems of classification and visualization of multidimensional parameter spaces are addressed.
3D User Interfaces: Projects concerned with applying virtual reality technology to cost effective and ergonomic desktop virtual environments. Two-handed interaction with tangible devices is the main research focus. This research is combined with the engineering of prototype desktop solutions together with several affiliated research groups.

Quantum Computing and Advanced Systems Research

Theme leader:
H.M. Buhrman

Quantum Computing: Research on quantum information and communication technology and processing, quantum algorithms, quantum communication complexity, quantum complexity classes, quantum cryptography, quantum information theory, and applications of quantum information theory to classical computing and physics.
MDL Learning and Algorithmic Statistics: Information theoretic methods for learning from data, Minimum Description Length (MDL), maximum entropy, pattern recognition, learning when all models are wrong, practical individual rate distortion theory, and applications and refinement of parameter free clustering and classification
Advanced Algorithms, Systems and Genomics: Kolmogorov complexity, computational complexity, distributed computing, and bio-informatics. In particular: new non relativizing separations in line with P vs NP problem, time limited Kolmogorov complexity, universal distributions, characterization of random strings, and symmetry of information. General lower bound techniques. Design and analysis of algorithms for distributed and parallel systems.

International and national research programmes

CWI participates in many national and international research projects.
This overview lists all major projects with their duration, partners, and CWI project leader(s).

European programmes

European Union

OMEGA: Correct Development of Real-time embedded in UML
2002-2005
Verimag, CAU, RU, Weizmann Institute, OFFIS, EADS Launch Vehicles, France Télécom, Israeli Aircraft Industries, NLR
F.S. de Boer

CC: Computation and Control
2002-2005
Verimag, Parades, ETH Zürich, Lund Univ. of Technology, EDF, ABB
J.H. van Schuppen

RESQ: Resources for Quantum Computing
2003-2006
Univ. Libre de Bruxelles, Univ. Paris-Sud, Univ. of Bristol,
Max-Planck Gesellschaft zur Forderung der Wissenschaften, UU, SZTAKI, Univ. de Genève, Univ. of Cambridge, Univ. of Gdansk
H.M. Buhrman

QAP: Qubit Applications
2005-2009
36 Partners from different countries
H.M. Buhrman

EU networks

ADONET: Algorithmic Optimization Discretization
2004-2007
Various partners: CWI is coordinator of the Dutch Consortium
M. Laurent

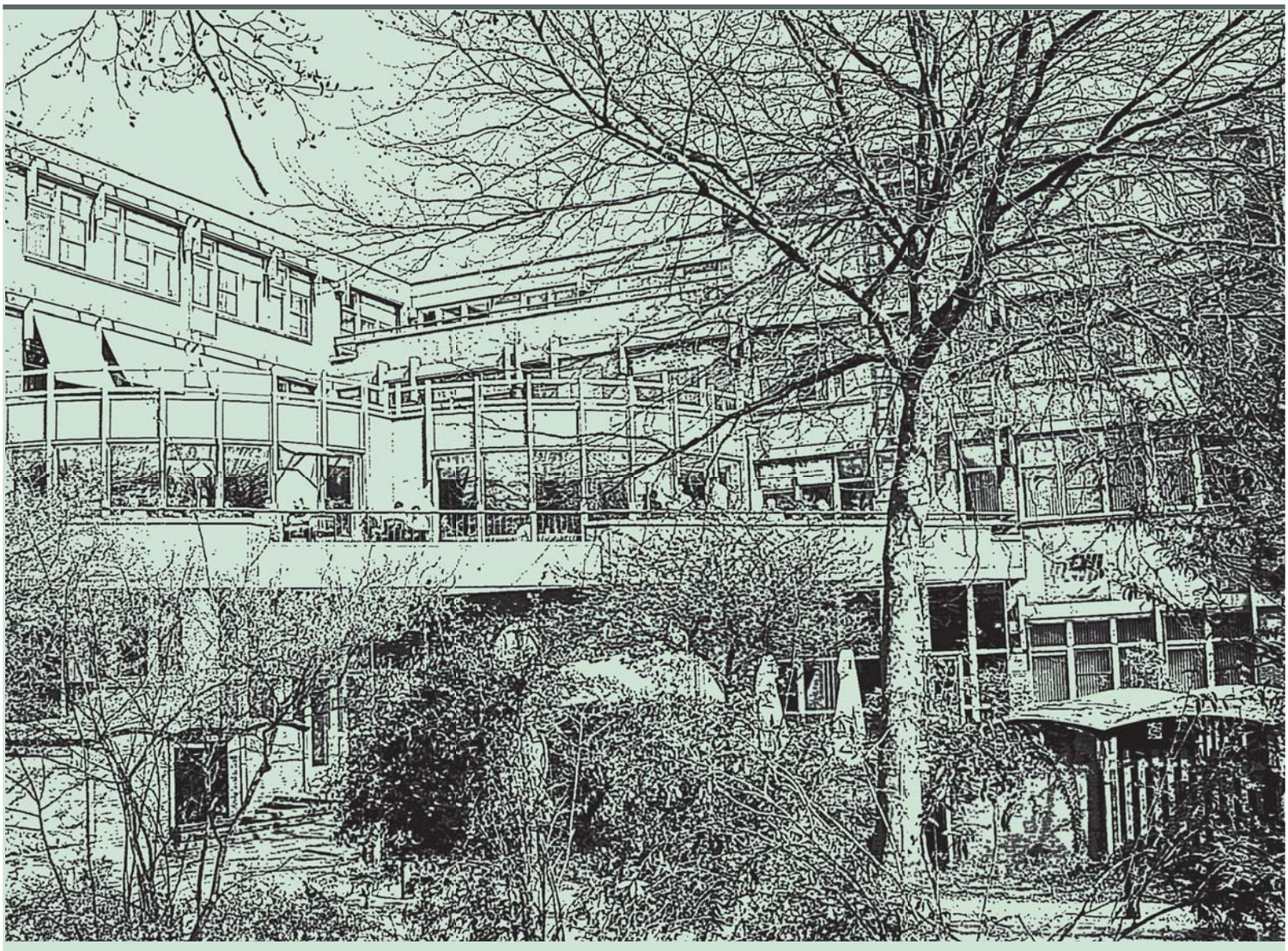
EuroNGI: Design and Engineering of the Next Generation Internet, Towards convergent multi-service networks
2003-2006
58 partners from different countries
M.R.H. Mandjes

BIOSECURE: Biometric for Secure Authentication
2004-2007
48 partners from different countries
B.A.M. Schouten

MUSCLE: Multimedia Understanding through Semantics, Computation and Learning
2004-2008
38 partners from different countries
E.J.E.M. Pauwels (scientific coordinator)

DELOS: Digital Libraries
2004-2008
60 partners from different countries
M.L. Kersten

PASCAL: Pattern Analysis, Statistical Modelling and Computational Learning
2003-2007
Univ. London, and 50 more sites
P.D. Grünwald



National programmes

NWO

SPCO: Semidefinite Programming and Combinatorial
Optimization
2002-2007
LAAS-CNRS, Univ. Klagenfurt, Univ. Rennes, TUD
M. Laurent

CIP: Constraint and Integer Programming Techniques
2002-2007
ERCIM, Univ. Victoria (Canada), Univ. Singapore, Brooklyn College
K.R. Apt

FDP: Foundations of Declarative Programming
2002-2007
UvA, VU
K.R. Apt

FAST: Large-deviations Asymptotics and Fast Simulation
2001-2005
Lucent Technologies, UT, VU
M.R.H. Mandjes

RAPS: Rare-event Analysis of Processor-Sharing systems
2004-2007
Lucent Technologies, TUE
S.C. Borst

Efficient flow-scheduling in resource-sharing networks with variable service rates
2005-2009
-
R. Núñez Queija

Coordination With Perfomance Guarantees
2005-2009
-
R.D. van der Mei

SOC: Mathematical Models of Biological and Physical Processes with Self-organized Critical Behaviour
2001-2005
VU, Wesleyan
J. van den Berg

Critical Percolation and Excitable Media
2005-2007
-
J. van den Berg

AGP: Spectral Analysis of Processes with Stationary Increments
2003-2007
VU
K.O. Dzhaparidze

Mathematical Aspects of Discrete Tomography
2002-2006
UL, FEI Eindhoven, Lawrence Berkeley National Laboratory
H.J.J. te Riele

Algorithmic Validation of Widely Used Cryptosystems
2004-2007
Microsoft, TUE, UL
H.J.J. te Riele

Deliver: Intelligent Software Management and Delivery
2003-2006
Exact BV, Planon BV, ChipSoft BV, VU
P. Klint

LPPR: Language-Parametric Program Restructuring
2004-2006
VU
J. Heering

Hefboom-project
2005-2009
Hogeschool Amsterdam, VU, UvA
J.J. Vinju

IT-VDS: Integrating Techniques for the Verification of Distributed Systems
2002-2005
TUE
J.C. van de Pol

TIPSY: Tools and Techniques for Integrating Performance Analysis and System Verification
2004-2007
TUE
W.J. Fokkink

Account: Accountability in Electronic Commerce Protocols
2004-2007
VU, UT
W.J. Fokkink

CBCS: Coordination-based Parallel Constraint Solving
2000-2003
PNA1, Univ. Nantes
F. Arbab

MOBI-J: Assertional Methods for Mobile Asynchronous Channels in Java
2001-2007
UL, Christian-Albrechts-Univ. Kiel
F.S. de Boer

CoMoLo: Coalgebra Modal Logic
2002-2005
UvA, KUN
J.J.M.M. Rutten

C-Quattro: Compositional Construction of Component Connectors
2004-2008
VU
F. Arbab, J.J.M.M. Rutten

MIA: Medical Information Agent
2004-2008
AMC, UM, TUE
J.A. la Poutré

ScaNN: Scalable Reinforcement Learning in Asychronous Spiking Neural Networks
2003-2007
Veni project
S.M. Bohte

Three-dimensional Simulation of Phytoplankton Dynamics
2001-2005
UvA
B.P. Sommeijer

Numerical Modelling of the Formation of Neuronal Connections of the Nervous System
2001-2005
Netherlands Institute for Brain Research (NIH)
J.G. Verwer

Mesoscale simulation paradigms in the Silicon Cell
2004-2008
UvA
J.G. Blom

3D-RegNet: Simulation of Developmental Regulatory Networks
2004-2008
UvA
J.G. Blom

Mathematics and Computation for the System Biology of Cells
2004-2008
UvA, TUE, VU, MAS2 (Van Schuppen)
J.G. Blom

Modelling of Developmental Regulatory Networks
2004-2008
UvA
J.G. Blom

CellMath: Mathematics and Computation for the System Biology of Cells
2004-2008
VU, UvA, TUE, MAS2 (Van Schuppen)
J.G. Blom

Geometric Numerical Methods for Continuum Mechanics
2002-2005
Veni project
J.E. Frank

Symplectic Integration of Atmospheric Dynamics: Long-term Statistical Accuracy for Ensemble Climate Simulations
2005-2009
-
J.E. Frank

Interactions of Pulses and Fronts
2005-2009
-
A. Doelman

NDNS-Nonlinear Dynamics of Natural Systems
2005-2009
-
A. Doelman

hp-Adaptive Methods for 3D Convection Dominated Flows
2001-2005
UT, TCD, RAS-UB
P.W. Hemker

Robust: Numerical Methods and Computational Technologies for Singularly Perturbed Multiscale Problems
2004-2006
TUE, MSU Moscow, RAS UB
P.W. Hemker

RPOS-Realization and control of national positive systems
2005-2009
-
J.H. van Schuppen

Computational Topology for Systems and Control
2005-2010
Vidi project
P.J. Collins

NUMLED: Numerical Methods for Leading Edge Dominated Dynamics
2002-2006
-
W. Hundsdorfer

MRPDE: Multirate Time Stepping for PDEs
2004-2007
-
W. Hundsdorfer

MBA-Moving Ionization Boundaries and Charge Transport
2005-2008
NWO/FOM (Dynamics of Patterns)
U. Ebert

CIRQUID: Complex Information Retrieval Queries in a DBMS
2003-2007
UT
A.P. de Vries

I^{2}RP: Intelligent Information Retrieval and Presentation in Public Historical Multimedia Databases
2002-2005
Rijksmuseum Amsterdam, RUG, UM, UL
L. Hardman

Quantitative Design of Spatial Interaction Techniques for Desktop Mixed-Reality Environments
2005-2009
TUE
R. van Liere

Quantum Computing
2004-2006
-
P.M.B. Vitányi

Universal Learning
2002-2005
HIIT Helsinki, Univ. London
P.M.B. Vitányi

ACAA: Average-Case Analysis of Algorithms
2002-2006
Univ. Waterloo, BSI
P.M.B. Vitányi

Quantum Information Processing
2004-2009
Vici project
H.M. Buhrman

Learning When All Models Are Wrong
2005-2010
Vidi project
P.D. Grunwald

Quantum Computing: Algorithms, Proofs and Tradeoffs
2005-2008
Veni project
R.M. de Wolf

STW

PHOTO-ID: Photo-ID for Cetaceans Using Shape Matching Methods
2004-2007
CML Leiden, Netherlands National Herbarium, UU
E.J.E.M. Pauwels, E.B. Ranguelova

SEQ: Sequential Point Processes
2004-2006
Centrum voor Milieukunde Leiden, Fom-AMOLF, ITC, Kapteyn Instituut, Philips Research
M.N.M. van Lieshout

Practical Approaches to Secure Computation
2005-2008
TUE, Philips Research Lab.
R.J. Cramer

Electric 'Fracture': Growth and Branching of Ionised Channels
2005-2007
TUE
U. Ebert

SenterNovem (including IOP)

EQUANET
2003-2005
Lucent Technologies, UT, TNO-ICT, TUE
M.R.H. Mandjes

BASIS: Biometric Authentication Supporting Invisible Security
2004-2009
UT, TUE
B.A.M. Schouten

IDEALS: Idiom Design for Embedded Applications on
a Large Scale
2003-2006
ASML, TUE, UT, ESI
A. van Deursen

TT-Medal: Testing Methodologies with Advanced Languages
2004-2006
LogicaCMG, ProRail, Improve QS, Fokus, Daimler-Chrysler, Nokia, VTT, Conformiq, Nethawk
J.C. van de Pol

CIM III: Cybernetic Incident Management
2003-2006
SEN4, TUD, VU, Almende, CMotions, Falck
F. Arbab, J.A. La Poutré

DEAL: Distributed Engine for Advanced Logistics
2002-2006
Almende, ERBS, VU, Groeneveld Groep, Post-Kogeko Transport Groep, Vos Logistics
J.A. La Poutré

Calce: Computer-aided Life Cycle Enabling
2003-2006
PinkRoccade Public BV, Software Improvement Group, VU
J. Heering

SPCI: Single Page Computer Intraction
2005
TUD, Backbase
A. van Deursen

IOP-EMVT: Space-mapping and Related Techniques for Inverse Problems in Magnetic Shape Design, with Application to an Electromagnetic Actuator
2003-2007
TUE
P.W. Hemker

IOP-EMVT: Stochastic Methods for Field Computations in EMC Problems
2004-2007
TUE
P.W. Hemker

Waterland
2001-2005
TI, UT, TNO-TPD, NOB, NOS
A.P. de Vries

Passepartout
2005-2006
Stoneroos, V2, INS2 en SEN5
D.C.A. Bulterman, L. Hardman

Trust4 ALL
2005-2007
Oce, RUL
F. Arbab

Near Field Virtual Reality Technologies
2005-2006
Gallium Europe, VOF
R. van Liere

Bsik projects

BRICKS: Basic Research in Informatics for Creating the Knowledge Society
2004-2009
TUD, TUE, UT, UU, NWO
J.K. Lenstra, J.G. Verwer

MultimediaN: Multined 12 Netherlands
2004-2008
CTIT, IBM, LogicaCMG, TI, TNO, TUD, UU, UvA, VU, V2-Waag Society
M.L. Kersten

VL-e: Virtual Laboratory for e-Science
2004-2009
see HYPERLINK "http://www.vl-e.nl" www.vl-e.nl about VL-e consortium partners
R. van Liere

Contract research

Stagesporen
1995-indefinite
VU, UM, UL
A.M.H. Gerards

Railway Optimization
1994-indefinite
NS Reizigers
A.M.H. Gerards

FLORIN: Flow-level Performance of Integrated 3G CDMA Networks
2003-2006
France Télécom
M.R.H. Mandjes

Beoordeling scripties IBM IT Architecten leergang
2005
IBM
R.D. van der Mei

DocGen: Documentation Generation
1999-indefinite
Software Improvement Group BV
A. van Deursen

Ambulant Mobile SMIL for PDAs
2003-2004
NL.net
D.C.A Bulterman

Ambulant NxG
2004-2006
NL.net
D.C.A. Bulterman

ASF: Asymptotics and Special Functions
1999-2005
Univ. Madrid, Univ. Pamplona, UvA, Abramowitz-Stegun group
N.M. Temme

ASF+SDF specificatie voor de expansie van RISLA
2005
Capgemini
M.J. van den Brand

Telematica Instituut projects

CHIP-Cultural Heritage Information Personalization
2005-2008
TUE, Rijksmuseum
L. Rutledge

Miscellaneous

Spinoza Award project
2005-2010
A. Schrijver

Parallel Implementation of a Coupling Interface for Fluidstructure Interaction
2005-2006
NCF Grant
B. Koren

STREAMERS-Moscow: Streamer Discharges: Experiments, Theory, Applications
2004-2007
NWO-RFBR programme (Russisch Nederlandse Samenwerking)
TUE, MIPT (Moscow), IVTAN (Moscow)
U. Ebert

Modelling and Inferring Developmental Regulatory Networks
2005-2008
NOW-RFBR Programme (Russisch Nederlandse Samenwerking)
UvA-section Computational Science, The Ioffe Institute of the Russian Academy of Sciences
J. Blom

Pictures and illustrations AR05

CWI/: 2, 5, 6, 7, 8 (right), 9, 11, 14, 16 (left, below), 17, 18, 19, 20, 23, 24, 25, 26, 29, 30, 32, 33, 34, 38, 41, 42, 44, 45, 46, 48, 49, 50, 55, 56, 57, 58, 59, 60, 61, 63, 67, 69, 71

Almende: 40 (upper)

AVC fotografie, Vrije Universiteit: 15 (right, below)

Hannie van den Bergh/Theater Adhoc: 30-31 (middle)

Eckart Bierdümpel: 28

Ernst van Deursen: 15 (upper right)

BED, Universiteit van Amsterdam: 37 (below)

ITEA: 10

Juan Guillen-Scholten: 19 (upper right)

J. Huisman: 36 (with permission from Nature)

Jeffrey Jonk: 40 (below)

KNAW / Henk Thomas: 16

Universiteit Twente/DACS: 21

University of Hawaii: 37 (upper)

Arie Wapenaar: cover, 8 (left)

Own pictures: p. 18-20 (Erika Abraham-Mumm, Dion Gijswijt, Miguel Valero Espada, Willem Jan van Hoeve, Carolynne Montijn)

Colophon

Published by: Stichting Centrum voor Wiskunde en Informatica, 2006
Production: Communications, Library and Information services (CBI), CWI
Text and editing: Annette Kik, Lieke Schultze and several scientists, CWI
Design, artwork & illustrations: Tobias Baanders, CWI
Photographs CWI: Tobias Baanders and Jan Schipper
Picture in cover illustration: Arie Wapenaar
Printing Grafisch Bedrijf Ponsen & Looijen bv, Wageningen