CWI

Centrum Wiskunde & Informatica

Annual Report 2015

At the moment of writing, we just celebrated the 70th anniversary of our founding in 1946. I am proud that we have been able to serve society with our research for such a long time. We have seen wonderful times: the invention of computers and the internet, the rise of computer science and the growing role of computational science and data-driven research.

Moreover, we can take pride in having a central role in all of these developments, and are still at the forefront of our ever-expanding field. I have high expectations of the QuSoft research centre that we launched in December 2015 together with UvA and VU to investigate algorithms, protocols and applications for future quantum computers. It has the potential to revolutionize the world of computing, just as the pioneers at our institute did in the early years of CWI. Considering the quality of our researchers and research topics, I am confident that we can make a very strong case for CWI in the Dutch research landscape, and that the past 70 years were only the beginning of the wonderful history of our institute.

In 2015, we have been able to add new achievements to our growing list of contributions to fundamental research and societal relevance. This Annual Report gives a summary of our efforts, and accounts for what we have done with the resources entrusted to us by society and our public and private partners. This document is intended to be browsed in no particular order. In it, you will find four articles where we highlight our research on smart energy networks, cryptanalysis, medical informatics and measuring user experience. In five overviews, we further present a bird's eye view of our work on the research themes Software, Information, Life sciences, Logistics and Energy. These texts are interwoven with snippets of information concerning other events and activities at CWI in 2015 and facts and figures about our institute.

I hope you will enjoy reading and browsing our Annual Report 2015.

Jos Baeten
General director

About Centrum Wiskunde & Informatica

Mission

Centrum Wiskunde & Informatica (CWI) is the national research institute for mathematics and computer science in the Netherlands and is part of NWO, the Dutch Science Council. The mission of CWI is to conduct pioneering research in mathematics and computer science, generating new knowledge in these fields and conveying it to trade and industry and society at large.

Vision

Results of mathematics and computer science are the invisible driving forces behind our economic growth and welfare, and are instrumental to developments in other scientific disciplines. They provide new insights and powerful tools for societal problems in energy, health care, climate, communication, mobility, security and many other domains. As the national

Research theme

Software

Interactive systems

Interactive systems with appealing visualizations are the hallmark of today's, mostly web-based, systems. Under the hood, their implementation is often complex, hard to extend and hard to maintain. There is a tension between ease of programming and a good runtime performance. Software engineers at CWI have addressed this problem by designing new functional programming abstractions for declarative and modular interactive systems. The new abstractions avoid known performance pitfalls of existing frameworks. As a result, interactive systems become easier to maintain, while exhibiting good performance.

Formal Methods Work

While trying to prove the correctness of the TimSort algorithm with formal methods, researchers at CWI unexpectedly found an error that crashes programs. TimSort is the default sorting algorithm in Android, Hadoop (Apache), and the programming languages Java (Oracle), Python and Go (Google). Their bug report with an improved version to fix the bug triggered changes to these frameworks and languages. The proof of the new version required over two million rules of inference and thousands of manual steps. The discovery attracted worldwide attention.

continued on p. 3

platform for mathematics and computer science CWI wants to expand its position in safeguarding the interests of these research fields and play a leadership role in science policy. To achieve this, CWI is in the forefront of developing new lines of long-term research in high risk areas, inspired by problems in society and industry. We also serve as a breeding ground for academic staff and young talented researchers, and give high priority to knowledge transfer. This is not only achieved by scientific publications and public lectures, but also through training PhD students to become high-potential researchers in science and industry, founding spin-off companies, collaboration with private and public partners and making innovative software tools available for researchers, companies and the general public.

Milestones

CWI has a unique talent pool of researchers. Since its foundation in 1946, more than 190 of its researchers have become **full professor**. In 2015, our researchers included a **Spinoza Prize** winner, 19 researchers with one or more **NWO Innovational Research Grants**, two **ERC Grant** holders and two **KNAW**-members.

CWI has a long-standing tradition of excellence in research that is both fundamental and societally relevant. CWI's track record includes building **the first computer in the Netherlands**, computing the **dike heights for the Dutch Delta Works**, connecting Europe to the **internet**, developing the **Python** programming language, computing the **train timetables for the Dutch Railways**, breaking factorization records of **RSA encryption** for internet security and developing the open source database system **MonetDB**. Recent highlights include launching the **QuSoft** research centre for quantum software, showing the **vulnerability of the SHA-1 standard** for internet security, developing proactive planning methods for **ambulance**, **firefighters** and **police services**, investigating **smart energy networks** and modelling and simulating phenomena such as **lightning**, **ocean currents**, **financial products**, **wind parks** and **proteins**.

CWI plays a central role in various programs and organizations, including the **W3C Benelux Office**, **Platform Wiskunde Nederland**, **EIT Digital**, **ERCIM** and **Informatics Europe**. Since its foundation CWI has commercialized its research in the foundation of **22 spin-off companies** that have generated millions of turnover to date.

Research theme Software

VideoLAT

Videoconferencing systems always have a delay from sender to receiver. As it affects human communications, this is a major factor in the quality of experience. Tuning a system to reduce the delay requires effectively and easily gathering delay metrics on a wide range of settings. To support this process, CWI developed the VideoLat software. It provides an innovative approach to understand glass-to-glass video delays and speaker-to-microphone audio delays. It is available as open source to enable extending and modifying it for different scenarios.

Quantum-safe cryptography

In the future, cryptography will be challenged by quantum computers and very high computing power. CWI researchers are working on security systems that cannot even be broken by quantum computers or unlimited computing power: information-theoretically secure multiparty computation. This fundamental research has interesting applications, such as auctions with secret bidding strategies and secure electronic voting. Last year, CWI and Aarhus University published a book on this topic, 'Secure Multiparty Computation and Secret Sharing'. This topic also featured prominently on the popular Wired website.

RDFa

RDFa, a W3C standard co-originating at CWI, defines markup for languages like HTML, XML and ODF, which adds machine-readable metadata to otherwise human-readable documents, making that metadata easy to extract and use. For example, search engines can identify a page as a product description, and other pages as reviews of that product, and bring them together when the product is searched for. Present on millions of web pages, RDFa is now used by companies like Facebook, Best Buy, and the coalition of major search companies (Google, Bing, Yahoo and Yandex), schema.org.

continued on p.2

Highlight

ICT against cancer

When deciding how to treat a patient, medical experts are often faced with difficult decisions that involve conflicting goals. Clinicians in radiotherapy encounter this when determining an irradiation plan for a specific patient to treat cancer. Because perfect plans are almost never possible, any irradiation plan will deliver dose to the tumour as well as to nearby healthy organs. As a consequence, an irradiation plan that may have a good chance of destroying the tumour may also have substantial risk of collateral damage to healthy organs. Making such decisions is difficult, but crucial for the success rate of medical procedures. In two new projects, both acquired in 2015, CWI will research and develop new ICT methods and techniques to provide better decision making support for medical experts in such cases. Lead scientist from CWI is Peter Bosman, who heads the Medical Informatics research line in CWI's Life Sciences group.

Research theme

Information

Big Data at high performance

Computer hardware systems have evolved into complex systems with a wide range of components such as spinning disks, SSDs, RAM, and CPUs. However, improvements in hardware technology have not resulted in a more efficient interaction when these various memory components work together on a certain task. Researchers at CWI investigate data management and analysis on such modern hardware and develop techniques to improve data processing performance significantly. The results are of interest for both scientists and companies that rely on fast data analysis for their research, business or services.

SKA Telescope

The SKA project is an international effort to build the world's largest radio telescope. It will eventually have over a square kilometre of collecting area and will generate vast amounts of data at 100s GB/s, which need to be processed in real-time. CWI and its spinoff MonetDB Solutions will develop technology to ensure that the system can sustainably handle growth in terms of query complexity and data volume. In addition, it will allow for safer addition of new features and performance improvements of the software and algorithms used in data processing, guaranteeing that they work as expected.

continued on p.5

Historic dose reconstruction

A large percentage (75%) of people that were successfully treated for cancer as a child is confronted with one or more adverse effects of the treatment later in life, such as radiation-therapy related cancer, heart or lung problems. Together with the department of Radiation Oncology of the Academic Medical Center (AMC) in Amsterdam, CWI will study and develop tools needed to understand the relationship between radiation dose and radiation-related long-term effects in survivors of childhood cancer. By investigating this relationship, ultimately better informed decision-taking can be realized when designing new treatment plans, potentially leading to less long-term adverse effects and reduced severity of these effects. This project is funded by the Foundation Children Cancer free (Stichting KiKa).

The study is based on the 3D-reconstruction of the radiation dose of former patients that were treated successfully more than twenty years ago and whose long-term effects are known. To analyse in detail the relationship between these effects and the radiation dose that former patients have received, a 3D dose distribution is required that indicates the exact location and quantity of the delivered dose. However, of these former patients only 2D image information (X-rays) is available which lacks crucial information to calculate the 3D dose distribution.

To solve this challenging problem, the researchers will match data from patients that have been treated in the past, with patients that have been treated more recently and of whom a 3D CT scan is available. Based on this match the dose distribution of the historic radiation plan is reconstructed in 3D after correcting the CT scan of the recently treated patient for small anatomical variations. This reconstruction enables the researchers to study the relationship between the radiation dose and the long-term effects in detail.

Bosman will develop the underlying learning strategy to match the patients. For this purpose, state-of-the-art machine-learning and optimization algorithms will be developed and deployed.

Improving internal radiotherapy

In a second project, Bosman will work on improving the medical software that is used for making treatment plans for internal radiation, also known as brachytherapy.

continued on p. 6

Research theme Information

Birdwatching at Rijksmuseum

The Rijksmuseum and Naturalis are currently in the process of donating large parts of their digitized collections of bird images to Wikimedia Commons. Amateur birdwatchers were invited to Rijksmuseum as citizen scientists to identify as many bird species depicted on these images as possible and record these. For this purpose COMMIT/ SealincMedia, a research consortium in which CWI is participating, has developed a dedicated online tool for the Rijksmuseum. With this tool, common and scientific names of species depicted in artworks can be recorded in an intuitive way.

Talk of Europe

In the 'Talk of Europe' project debates of the European Parliament are published as Linked Open Data. The result is an online accessible database of what is said in the plenary meetings of the European Parliament, with translations in 22 languages, including names of politicians, the countries they represent and the national and European parties and committees they are a member of. The combination of linked datasets with the base available in 22 languages should allow research questions not yet feasible. As such, interlingual comparative research through digital tools becomes possible.

Statistics for big data

By desiging a data management system focused on statistical and analytical models, analysis of big data could be strongly improved and sped up. CWI investigates whether such models can be used to replace data storage, and how to use these for high-accuracy responses to queries. The database management system consists of an integration of MonetDB and statistical programming language 'R'. This research is funded by the Veni grant of Hannes Mühleisen, obtained in 2015.

continued on p.4

Medical Informatics

Researcher Peter Bosman of CWI's Life Sciences group heads CWI's research line in Medical Informatics, which applies computer science and mathematics in medicine. He specializes in metaheuristic algorithm design, oftentimes for multi-objective optimization: finding optimal solutions in cases where several conflicting goals have to be optimized simultaneously. To obtain high-quality solutions for (real-world) optimization problems, Bosman in particular focuses on the design of metaheuristics that combine machine learning, evolutionary algorithms, and problem-specific heuristics.

Brachytherapy is an important form of radiotherapy, mostly used to treat cancer, where catheters or applicators are placed near the tumour and through which a radioactive source is led. The delivered dose by the source is determined by how long it is stopped at a certain position. This dose distribution is essential: inside the tumour area the radiation needs to be high, but outside it has to be minimal to prevent damage to healthy tissue. To realize this, special software is used that assists medical experts in determining a radiation plan that indicates how long the source must stop at different locations, based on images (3D CT or MRI scans of the tumour and its surrounding area).

With the current software a lot of time-consuming manual effort is required to construct a radiation plan that represents a clinically acceptable trade-off between desired effects and possible side effects. The researchers want to apply novel developments in fundamental computer science and artificial intelligence to improve this situation. The new software should be able to learn from previously approved plans what is likely to be a good plan for a new patient. Moreover, the software should present the therapist with multiple interesting alternative options for radiation plans. By quickly navigating alternative plans, the therapist can make a well-informed decision, with the ultimate goal of improving the quality of life of cancer patients.

The project is a collaboration between CWI, the department of Radiation Oncology of the Academic Medical Center (AMC), and Elekta Brachytherapy, the biggest manufacturer in the sector worldwide. The project is funded through the Innovative Public-Private Partnerships in ICT – Technology Area (IPPSI-TA) programme of the Netherlands Organisation for Scientific Research (NWO).

Research theme

Life sciences

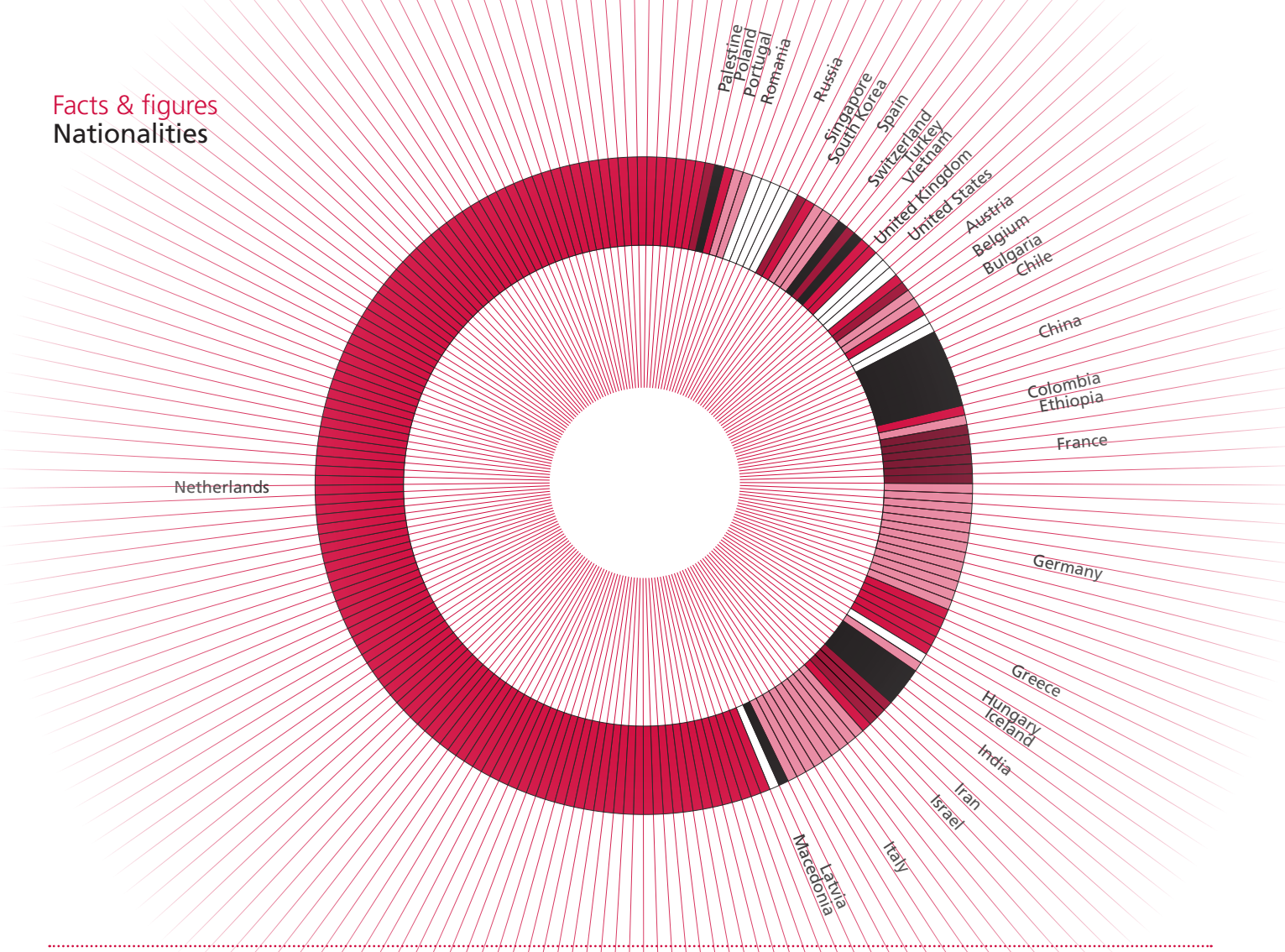
Working memory

Scientists understand how neurons, the smallest computational units of the brain, behave during tasks, but it is unknown how brains learn to make efficient choices, in particular when the brain's working memory is involved. This working memory is an essential part of intelligence that has been studied for a long time. CWI has developed a biologically plausible neural network model that can learn to remember past events in order to use them in the future. To develop their model, the researchers created a parallel with complex animal behaviour-learning through reinforcement learning.

Predicting drug trial results

In drug trials, researchers investigate the effect of potential new drugs by administering these to model organisms, such as mice. If an effect is found, the drug is tested on a small set of humans. Only 25% of the experiments pass this phase, mostly because the results found in animals turn out to be non-transferable to humans. CWI works on mathematical models for predicting transferability by comparing gene activity patterns of organisms. These predictions could reduce the number of lab animals needed in drug trials and help directing lab research towards more transferable experiments.

continued on p.7



Research theme Life sciences

Reducing radiation dose

X-ray computed tomography (CT) is a powerful tool for non-invasive cardiac imaging. However, radiation dose is a major issue. CWI and the University of Antwerp jointly developed a reconstruction method that reduces the radiation dose without compromising image quality. This is achieved by exploiting prior knowledge of stationary and dynamic regions in and around the measured organ. Experiments on simulation data and cardiac images of mice show that, with comparable image quality, the radiation dose can be substantially reduced compared to conventional protocols.

Vascular growth

Vascular growth involves two types of cells: tip cells that lead the growing sprout and stalk cells that follow behind. During growth, tip and stalk cells play leapfrog, changing position at the growing tip of a vessel sprout. Experimental biologists could not agree on the functionality of this process and on its mechanism. Simulations of CWI now show that this leapfrog behaviour might be a side-effect of the mechanism of vascular growth. Also, the model illustrates how cross-talk between gene activity and cell-cell signaling can determine the cell's position in the blood vessel sprout.

Personalized medicine

Genetic differences between humans can for a large part be attributed to structural variation in the human genome. CWI researchers have contributed to a first-ever large-scale reference panel, a statistically organized list, for structural variations found in the Genome of the Netherlands project. This means that these genetic variations can now be used in genome-wide association studies, linking structural variances in the human genome to disease risks and the expression of diseases. This is a major step up in the direction of personalized medicine.

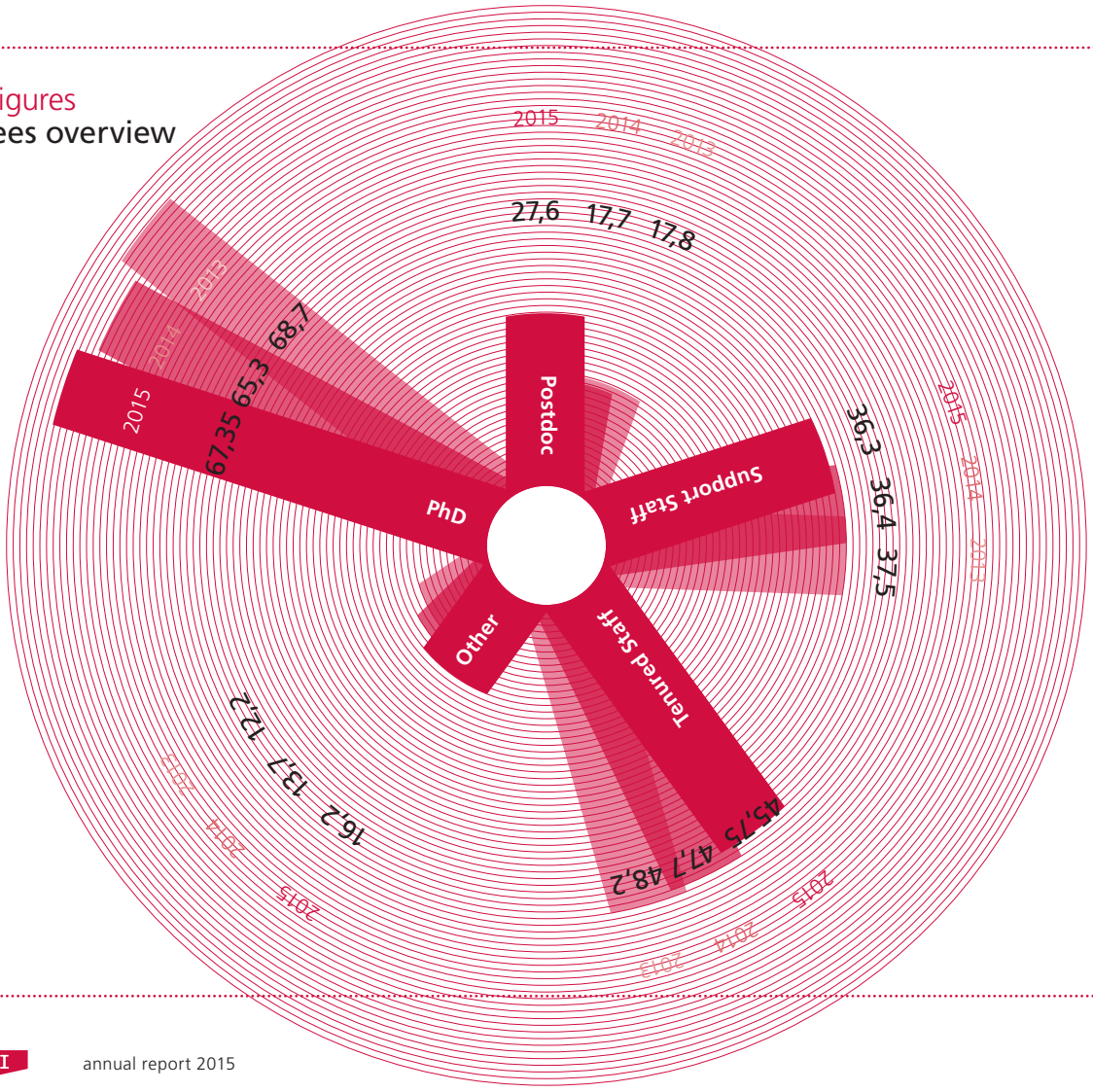
continued on p.6

Smart grids: saving money on sunny, windy days

Our future energy system will mainly consist of renewable energy sources such as sun and wind. A major drawback of these natural sources is that the weather determines how much energy is available at any moment. Another complicating factor is the expected rise of electric vehicles: charging these will take a heavy toll on the energy grid. To remedy this shift in supply and demand, researchers of the Intelligent Systems group at CWI are working on demand response: automatic shifting of demand to dampen both peaks and troughs.

The Intelligent Systems group at CWI consists of both computer scientists specialized in game theory and electrical engineers with knowledge of power grids. Together, they are investigating possible infrastructures for power supply in a world depending on renewable energy. Their research focuses on smart grids: intelligent energy grids that use various mechanisms to balance supply and demand. An example is reducing the demand for electric vehicle charging at the end of a workday by lowering

Facts & figures
Employees overview



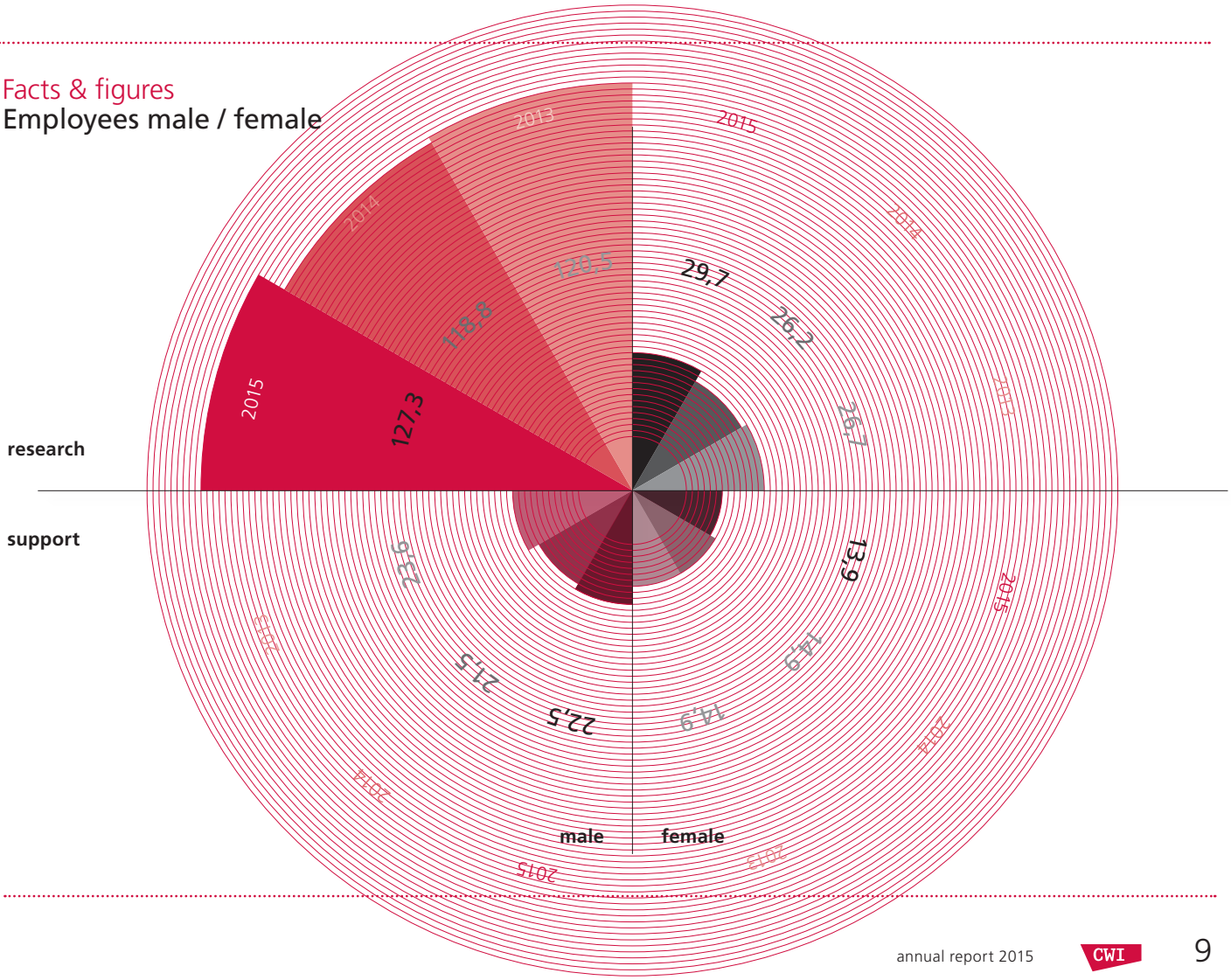
prices during off-peak hours. Depending on individual settings based on the owner's preferences, the car could automatically decide to defer charging to times at which renewable energy is abundant and prices are low. During sunny or windy hours energy prices would be very low, which would be the perfect opportunity for business and households to carry out any process with high energy consumption. The group investigates the consequences of market design choices on the energy market and grid, showing how such smart grids would work in practice.

Electric Vehicle Aggregator

In a demonstration case, the researchers are focusing on charging flexibility of electric vehicles in Amsterdam. Felix Claessen, researcher in the Electric Vehicle Aggregator (EVA) project, says: "In Amsterdam there are currently around 6000 electric vehicles, while over 2000 homes and businesses have installed solar panels. This creates an interesting opportunity to start matching demand and supply on a local level to avoid network congestion." The researchers apply evaluation tools to demonstrate the consequences of various infrastructure and market designs on the operation of the Amsterdam grid. "These simulations can be used to support business models," says Claessen. "For instance, we considered a taxi company that operates a fleet of electric vehicles. By implementing a charging strategy that takes advantage of fluctuating market prices, this company could charge their vehicles cost-effectively when renewable energy supply is high and demand low. Generally, we found opportunities for a favourable business case for this type of business model." EVA's business model is evaluated in a simulated Dutch energy market for the urban area of Amsterdam with fast-charging stations. The project initiated from the European Virtual Smart Grid Lab within EIT Digital, the European Institute of Technology and Innovation for fostering digital technology innovation and entrepreneurial talent in Europe. Felix Claessen is currently investigating the potential for a spin-off company for business models such as EVA. For 2016, EIT Digital has granted a pilot project in which the aggregation service is tested with cars and an energy retailer in Berlin. This includes a subgrant to start the company. The start-up will initially offer a consultancy service as the market for this type of application matures.

CWI produced a video on EVA, which can be viewed at www.cwi.nl/eva

Facts & figures
Employees male / female



cwi in 2015

Amsterdam Economic Board

On 13 March 2015, deputy mayor and alderman of Amsterdam, Kajsa Ollongren, paid a working visit to CWI to get acquainted with our research. She saw some highlights of CWI research, including our work on smart energy and quantifying user experience, and participated in a demonstration in the Pampus experimentation lab.

cwi in 2015

W3C Benelux Office

The W3C Benelux Office, which is hosted by CWI, welcomed three new members in 2015: De Nederlandsche Bank, ISO 20022 Registration Authority and Sirris. The Office co-organized a number of events, including the Internet New Year's event for 450 visitors, a WebRTC masterclass with ISOC.nl and WebRTC Nederland, an HTML5 Web Apps workshop with ISOC.nl and Waag Society, and an XForms Day prior to the XML Amsterdam conference.

cwi in 2015

Professorships

The following CWI researchers acquired a new position as a professor in 2015

- Lynda Hardman (Professor of Multimedia Discourse Interaction at Utrecht University)
- Marie-Colette van Lieshout (Professor of Spatial Stochastics at University of Twente)
- Bert Zwart (Professor of Stochastic Operations Research at the Eindhoven University of Technology)

continued on p.11

QuSoft research centre for quantum software launched

On 3 December 2015 CWI, UvA and VU launched QuSoft, the first research centre dedicated to quantum software. The mission of QuSoft will be to develop new protocols, algorithms and applications that can be run on small and medium-sized prototypes of a quantum computer.
The main focus will be on the development of quantum software, which requires fundamentally different techniques and approaches from those to develop conventional software because of the counter-intuitive quantum mechanical properties of the quantum computer such as superposition, interference and entanglement. A fundamental driving research question is to develop software and find applications that exploit the extraordinary power of quantum computers. The institute will be headed by Harry Buhrman (CWI), with Kareljan Schoutens (UvA) als co-director. The new centre builds on these institutions' excellent track record in quantum computing and quantum information.
QuSoft will specifically target the research fields of few-qubit applications, quantum testing and debugging, and quantum architectures. In addition, the centre will cover the related field of quantum cryptography.
Harry Buhrman: "The launch of the QuSoft research centre is great news. It allows us to scale up our work on applications and software designed to run on the kind of quantum computer hardware that seems to be just around the corner. Investment in the science and development of quantum software is vital, as at present no-one really fully understands how to properly exploit these special opportunities quantum hardware will bring."
In addition to investments by CWI and VU, QuSoft receives structural funding through UvA's research priority area Quantum Matter and Quantum Information (QM&QI). The new centre will be hosted by CWI. It aims to grow to 35 to 40 researchers and will be home to four research groups.
QuSoft was launched during the CWI Lectures on Quantum Computing, which featured world-renowned experts such as Gilles Brassard, Ronald Hanson, Richard Jozsa, Serge Massar and Mario Szegedy.

cwi in 2015

Harry Buhrman in Universiteit van Nederland

In January 2015, the Universiteit van Nederland published a video series of five public lectures by CWI researcher Harry Buhrman on quantum computers. The quantum computer is viewed as one of the most promising technologies of the 21st century. It uses the effects from quantum mechanics for computation. Buhrman introduced viewers to the basic concepts and the do's and don'ts of this new technology. The Universiteit van Nederland creates short and visually appealing online lecture series of the best researchers in the Netherlands. The lectures attract tens of thousands of viewers.

continued on p.10

cwi in 2015

Awards and honours

A selection of awards and honours received by CWI researchers in 2015:

- Van Dantzig Prize (Bert Zwart)
- Software Engineering Distinguished Service Award (Paul Klint)
- EURO Gold Medal (Lex Schrijver)
- LODLAM Open Data Prize (PoliMedia project, Laura Hollink)
- A.W. Tucker Prize (Daniel Dadush)
- Nominee Volvo Design Challenge (DIS group with ByBorre)

cwi in 2015

CWI in Bedrijf 2015: Everything Smart

The 2015 edition of CWI in Bedrijf was organized around the theme Everything Smart. All research themes presented their smart technology in demonstrations on the matchmaking market. Key note speakers included mayor Rob van Gijzel of Eindhoven, textile designer Borre Akkersdijk and Dutch figurehead for ICT René Penning de Vries. The event was concluded with the première of 'Remembering ARRA' , a short documentary produced by Google on the early days of Dutch computing and the development of the first Dutch computers at CWI (then called Mathematisch Centrum).

Highlight

Measuring user experience

We live in a society based on experiences. Whether we visit a theatre show or interact on social media, our experience plays a crucial role in our behaviour. Yet, it is surprising to see how little is actually known about how audiences value these experiences. The high-end technical solutions for shaping experiences sharply contrast with the rather conventional mechanisms used to measure them. The Distributed and Interactive Systems (DIS) group of CWI uses biosensor technology to quantify audience experiences and better understand their behaviour on a group and individual level.

"Back in 2012, we noticed the lack of adequate mechanisms to gather reliable and fine-grained feedback from audiences attending performing arts events," says Pablo Cesar, group leader of DIS. "We started to explore this area within an EU-funded

Research theme

Logistics

Lattice structures

Lattices are regular spatial arrangements of points with many applications. They are applied, for instance, in noise tolerant encodings for wireless cell phone messages and securing internet communications by hiding messages within high dimensional lattices. CWI works on the design of new cutting edge methods for efficiently utilizing lattice structures. This research is funded by the Veni grant of Daniel Dadush, obtained in 2015.

Rare events

Understanding low-probability events with a major impact such as floods, power outages and stock market crashes is challenging, as it is hard to obtain data from either real-life situations or large scale simulations. Researchers at CWI will develop a general framework for analysis of these rare events, developing robust algorithms for computation, estimation and simulation and applying these techniques to several major problems, such as the robustness of energy grids based on wind and solar energy. This research is funded by the Vici grant of Bert Zwart, obtained in 2015.

continued on p.13

project, Vconect. Using wearable sensors that measure galvanic skin response, the amount of sweat secretion which is an indication of emotional arousal, we were able to collect a continuous bio-data stream aligned with the experience of users. We found that this project attracted considerable attention in the media and art world, and soon became involved in various experiments."
During the last years, the group has developed know-how, infrastructure and algorithms for inferring user experience from raw bio-data streams. Cesar: "Our infrastructure consists of sensors that can be easily worn and are customizable for any type of person and environment. We deploy an ad-hoc network that allows robust real-time delivery of sensor data from the sensors to a central server using free-band radio technology. Our algorithms are included in this server and can process the data offline or in real-time, quantifying the user experience of the individuals and groups of people. The results can then be visualized

November 2015: War Horse in Shanghai (with the National Theatre of China)

In 2014, CWI started a cooperation with the Chinese news agency Xinhuanet to set up a user experience lab in China and to explore together biosensor technology and engagement. Through this partnership, the group came into contact with the National Theatre of China, which showed great interest in the biosensor research. In the fall of 2015, this resulted in a large-scale experiment to collect physiological responses of audiences during the acclaimed theatre production *War Horse*. CWI sent a team of the DIS group to facilitate the experiment in Shanghai.
The experiments involved putting small electrical galvanic skin response sensors on the fingers of spectators during the theatre performance, which measured the audience's alertness. The National Theatre successfully conducted the experiment over five days of War Horse performances. Valuable data from more than 150 participants was collected using the biosensors, including Chinese celebrities such as TV show hosts and playwrights. The experiment was well-received by the participating audience. The production team of War Horse used the results to find out whether adapting a British award-winning play had a similar effect on the Chinese audience as on the British audience, and whether adult and children, male and female, and audience with different interest in theatre responded differently to the *War Horse* performance.

continued on p. 14

Research theme Logistics

Prediction of charging stations

CWI can predict the demand for electric vehicle charging stations, using socio-economic features of neighbourhoods. Based on an extensive log of behavioural data, population and land use characteristics and charging probabilities, researchers can calculate the utility of charging stations in every neighbourhood, thus being able to advise the municipality of Amsterdam where to focus their expansion activities. With their results, the scaling-up is more effective. The capital city of the Netherlands wants to proactively increase the number of charging stations from over 1000 to 4000 by 2018.

Bus scheduling

In cooperation with software developers and bus operating companies, CWI is developing algorithms for small and large bus companies that are active throughout the Netherlands and Europe. By combining mathematical techniques from operations research and combinatorial optimization, even the most complicated constraints (such as European restrictions on the driving times and rest periods for bus drivers) can be taken into account. While practitioners usually spend weeks on constructing feasible timetables, these algorithms produce such a timetable in only seconds, and further qualitative results are even more promising.

Experiments on Optimal Pricing

Price experimentation is important for firms to find the optimal selling price of their products. Since experimenting with selling prices can be costly, it should be done right. A pricing policy should optimally balance between learning the optimal price and gaining revenue. CWI researchers proposed such a policy: controlled variance pricing (CVP). The methods starts seeking outside the normal prices and leads to both an optimal price and an upper bound on lost money. Numerical tests indicate that CVP performs well on different models and time scales.

continued on p.12

June 2015: Wearing Sense in Amsterdam (with ByBorre)

On occasion of the *CWI in Bedrijf* event on 4 June 2015, the DIS group demonstrated that sensor technology does not have to be intrusive. An unique collaboration between CWI and the Dutch textile designer Borre Akkersdijk (ByBorre) resulted in a live experiment in which biosensor data was transmitted from wearable devices. Borre gave a lecture wearing a special sweater incorporating heart rate sensors and accelerometers that helped gauge his own energy level. Part of the audience members also wore sensors. On a big screen, the audience saw a live stream of the engagement of the speaker and the public. Also in front of the room there was an installation by artist Lilia Perez, in which a series of balloons were linked to the reactions of audience members. If this person was not engaged, the balloon went down to a needle and popped. Luckily, no balloons were popped that day.

in the most adequate manner, depending on the application."
Cesar believes that they have only touched the surface of what is possible. "Our algorithms are now optimized for audiences attending an event, but they are customizable to other areas. We are aware that there are several domains such as marketing, tourism, internet and leisure, politics and music events that offer big opportunities to introduce these technologies. We are currently looking for long-term partnerships with the right partners who can help us to customize our technology to new application domains. I believe that we are only at the beginning of this journey and that the best is yet to come."

February 2015: Dance Event in The Hague (with Holland Dance)

In the winter of 2015, the DIS group measured the response of the audience attending the dance show *How long is now* by the Italian dance group Balletto Civile, at the Lucent Theatre in The Hague. Spectators could volunteer to be equipped with a biometric sensor and an accelerometer to monitor their reactions. The researchers used this data to automatically detect how and when the audience reacted to the dance performance. The experiment was done in cooperation with VU, UvA and TU Delft.

cwi in 2015

One Vici, two Veni's

In 2015 CWI received one NWO Vici grant and two NWO Veni grants. A Veni allows researchers who have recently obtained their PhD to conduct independent research for three years. A Vici grant allows researchers at a later stage in their career to develop their own research group for five years. They were awarded to:

- Daniel Dadush (Veni, for efficiently utilizing lattice structures)
- Hannes Mühleisen (Veni, for statistical models for big data analysis)
- Bert Zwart (Vici, for rare event simulation)

cwi in 2015

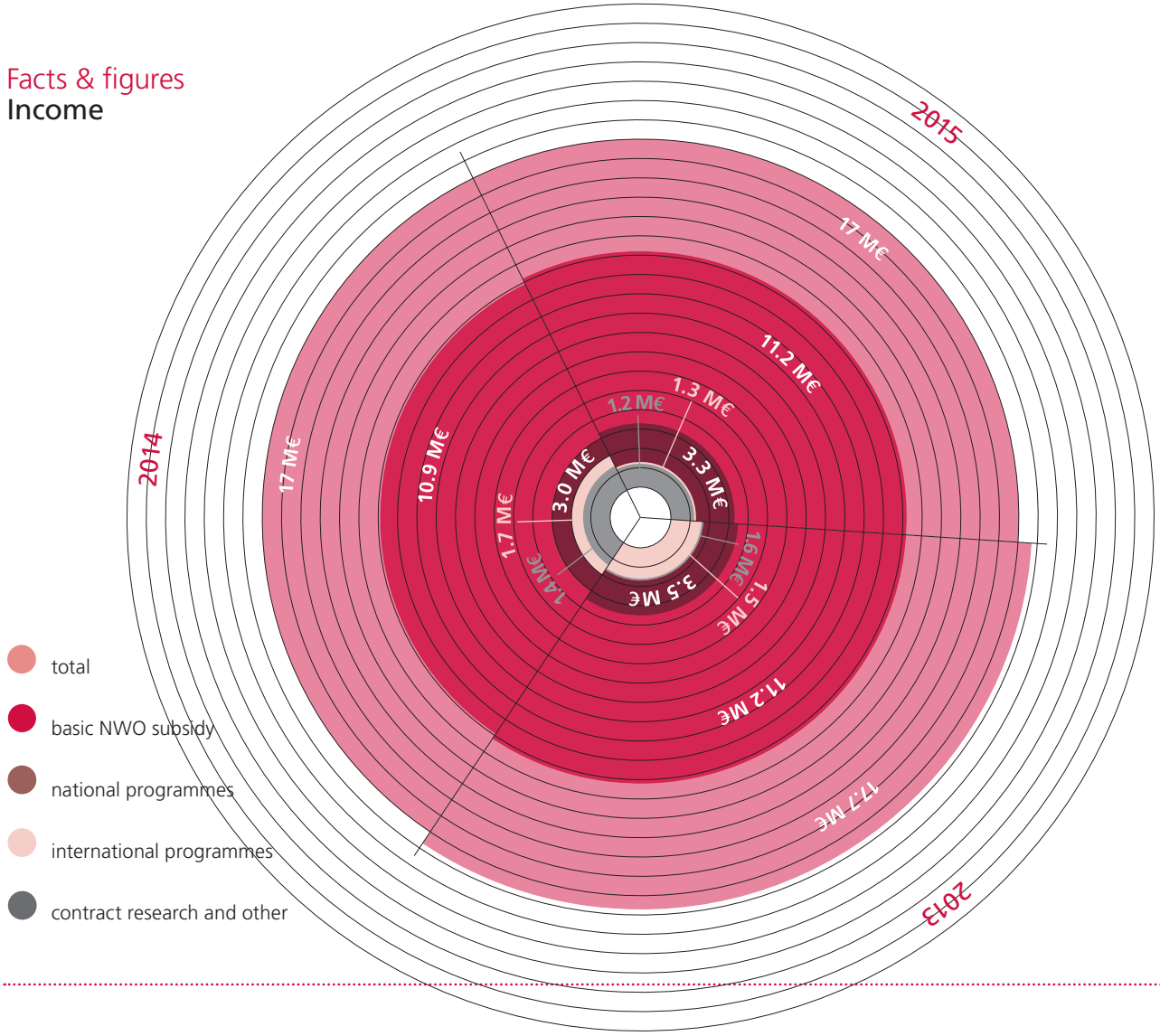
Lynda Hardman President Informatics Europe

Lynda Hardman (CWI MT member and senior researcher in the Information Access group) has been elected President of the Board of Informatics Europe, the European association of computer science departments and research laboratories. Hardman has already been serving as member of the Informatics Europe Board since 2012. As president of Informatics Europe, she aims to increase the quality of informatics research, ensure that educational innovations can be more easily disseminated, and strengthen the development of commercial cooperation across Europe.

cwi in 2015

Python 25 year anniversary

In 2015 it was 25 years ago that Guido van Rossum started developing the Python programming language at CWI. He designed Python in December 1989 and finished the first working draft in early 1990. Python is now one of the most popular computer languages worldwide. The anniversary was covered by several media, including the website of ACM, NRC, nrc.next and De Kennis van Nu (Radio 5). Tech website Tweakers recorded a special movie on Van Rossum for their web series 'Polderpioniers' with Van Rossum at CWI.



cwi in 2015

Media appearances

A publication on the origin of lightning in July attracted considerable media attention. In October the international press picked up on the urgent warning of CWI cryptanalysts and colleagues that the SHA-1 internet security standard should be retracted. The launch of the QuSoft research centre in December was widely covered by national media, including de Volkskrant, Trouw, nu.nl and Parool. Other highlights include an item on the Flemish tv show 'Iedereen Beroemd' (VRT), a long interview with director Jos Baeten on BNR Radio and the appearance of Ute Ebert in the tv show 'Lekker Weertje'.

cwi in 2015

NWO Transition

In 2015 a large-scale transition for the NWO organization was launched to make NWO more effective, respond more flexibly to developments in science and strengthen collaboration within science and with society. The current science divisions will be clustered in four domains, and all NWO institutes will be united in a single institute organization. As a NWO institute, CWI is closely involved in this process and made various contributions to the work groups charged with the elaborations of the plans.

cwi in 2015

Open access

CWI is actively involved in the open access movement. Starting in 2015, open access publishing is mandatory for all CWI publications, either through fully open access journals (golden road) or through offering to pre-print versions (green road). CWI also contributed to a report on open access for the European Research Consortium for Informatics and Mathematics (ERCIM) general assembly, which provides a series of principles and recommendations concerning the publication and dissemination of scientific output for all ERCIM members.

Highlight

A safer internet with cryptanalysis

CWI cryptanalyst Marc Stevens broke the core of the SHA-1 internet security standard together with an international team in 2015. This was much earlier than international security experts expected and gained a lot of media attention. The team urged the industry to retract the standard earlier. Their results ensured that an industry ballot to extend the issuance of SHA-1 certificates was withdrawn. This has made the internet safer.

SHA-1 is a cryptographic algorithm that was designed by the NSA in 1995 to securely compute message fingerprints. It became an industry standard that is commonly used for digital signatures, which secure credit card transactions, electronic banking and software distribution. It is fundamental to internet security, such as for HTTPS (SSL/TLS) security.

Research theme

Energy

Nuclear fusion

The plasma inside a nuclear fusion reactor of the tokamak type is prone to instabilities. The future of nuclear fusion as an energy source depends to a large extent on methods to control these instabilities. CWI and DIFFER develop and use computational methods to understand the plasma's dynamics inside the reactor. Standard computational methods are not equipped to deal with the plasma's extreme conditions, such as the very uneven spread of temperature and magnetic field. The researchers have developed novel computational methods to deal with the latter, improving the accuracy of simulations.

Reliable energy grid

Renewable energy increasingly contribute to the electrical grid. Although the transition to a sustainable power supply is desirable, it poses several challenges to grid stability. Renewable sources such as wind and sun are very variable, increasing the risk of current overloads and voltage deviations. Also, power generation is distributed over countless small turbines and solar panels, making steering mechanisms such as switching power plants on and off much less effective. CWI develops new simulation methods that can determine the stability of power grids under these circumstances.

continued on p.17

SHA-1 is a so-called hash function. It generates from input, such as text or code, a short string of letters and numbers (a hash), which serves as a fingerprint for that message. Even a small change in the input, like changing one letter in a message, will generate a very different and unpredictable output. When two different messages lead to the same hash, this is called a collision. Such collisions allow forgeries of digital signatures – a catastrophe for banking transactions, secure e-mails, and software downloads. The industry standard was already theoretically broken in 2005 but it had been difficult to make a practical attack for a long time. However, Stevens combined his advanced mathematical methods with techniques from fellow cryptographers to speed up the computations. In September, this joint effort by CWI, Inria and NTU Singapore – also known as 'the SHAppening' – led to a successful so-called freestart collision attack on SHA-1, breaking the full inner layer of SHA-1. By using graphics cards for their computations, the attack was made much more cost efficient. The researchers – Marc Stevens (CWI), Pierre Karpman (Inria and NTU Singapore) and Thomas Peyrin (NTU Singapore) – then estimated that a full SHA-1 collision would cost only between 75,000 and 120,000 dollar renting Amazon EC2 cloud over a few months, in early autumn 2015. This implied that collisions were already within the resources of criminal syndicates, almost two years earlier than previously expected, and one year before SHA-1 would be marked as unsafe in modern internet browsers in January 2017, in favour of its secure successor SHA-2. The team therefore recommended that SHA-1 based signatures should be marked as unsafe much sooner. In particular, they strongly urged against a proposal to extend issuance of SHA-1 certificates with another year in the CA/Browser Forum, for which the voting was scheduled briefly after the announcement. The proposed extension was not just because some companies were not ready yet, but also due to the fact that millions of users with old software, mostly from developing countries, would not be able to access some websites anymore. However, due to the shown insecurity, the proposal for extension was withdrawn

continued on p. 18

Research theme Energy

Valuing uncertainties

Cost-benefit decisions are often made for events happening in the future. These usually involve inherently uncertain aspects, such as the development of interest rates or even the global temperature. Using advanced mathematical techniques, financial mathematicians at CWI model and value such uncertainties. The results can be applied to financial and economic forecasts, such as to questions related to the long-term economic effects of climate change for various temperature change scenarios. PhD student Marjon Ruijter graduated with honours (cum laude) on this topic in applied mathematics.

Better 3D modelling of discharges

CWI made major progress in modelling the early stages of electric discharges, as they occur in lightning, high voltage electricity nets and plasma technology. Researchers developed computer models that allow for studying the development in full 3D within hours, while up to now one had to wait weeks or months, or in many cases computations were not possible at all. The results were used to model for the first time the rare growth of discharges perpendicular to the electric forces, caused by an abundance of free electrons in that direction.

Start of lightning

Researchers of CWI demonstrated in a Physical Review Letters article that lightning could be triggered by high energy particles from space, originating from supernovae. This is a big step in solving the mystery of lightning initiation. The particles - or 'cosmic rays' - produce a huge shower of electrons in the atmosphere. When the electrons reach the tip of a large hailstone, where the electric field is amplified, then lightning starts. Modelling the many processes at different scales in space, time and energy is very complex.

continued on p.16

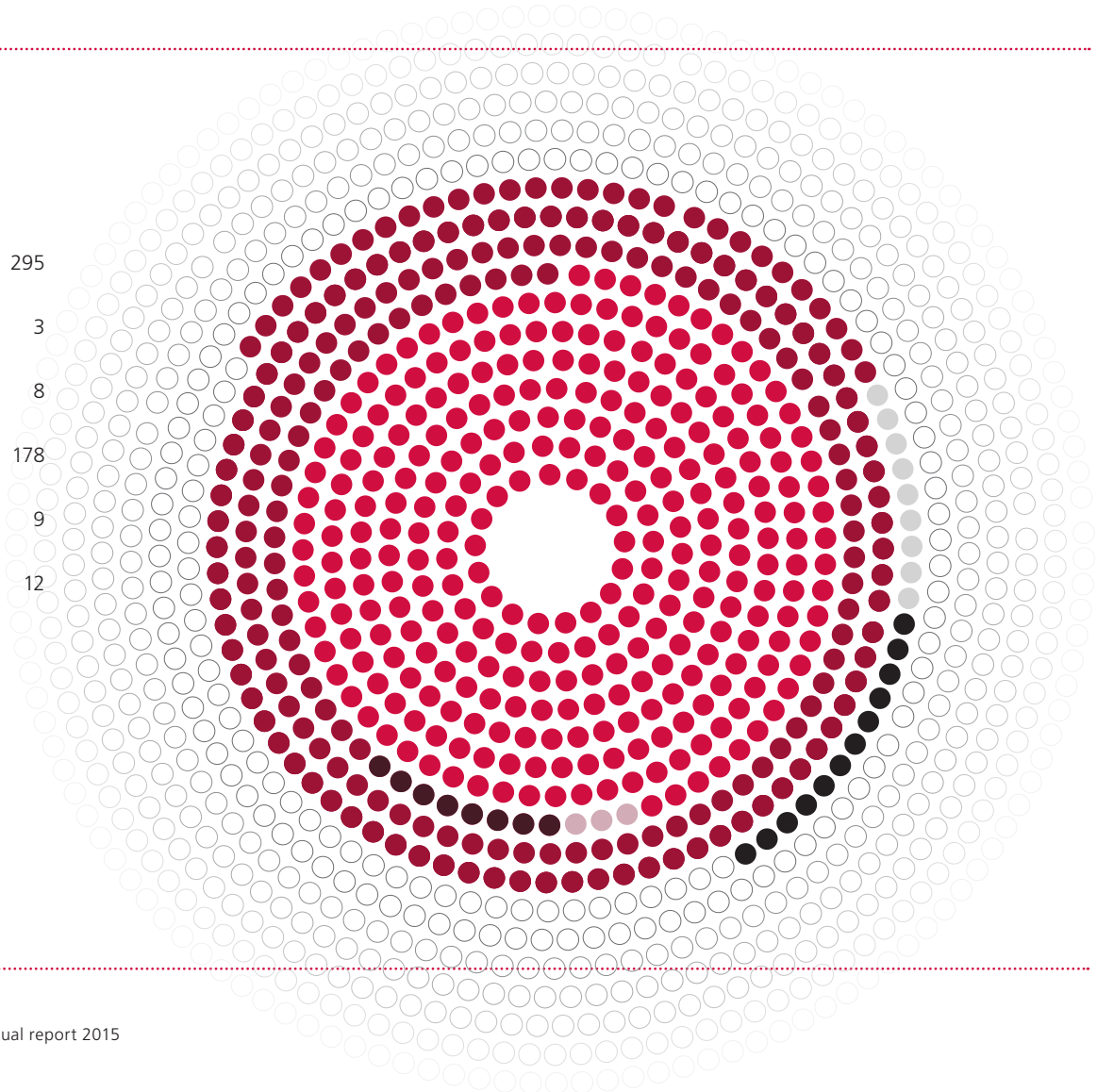
Cryptology at CWI

CWI has a long history in cryptography and cryptanalysis. Cryptanalyst and tenure track researcher Marc Stevens also broke the MD5 internet security standard for https in 2008 and analyzed the Flame super malware in 2012. He works in the Cryptology group at CWI headed by Professor Ronald Cramer, a leading international research group in this field. Its research is focused on foundational and practice oriented cryptology, in particular secure computation, public key cryptography, interactions with algebraic geometry, number theory, coding theory and combinatorics, cryptanalysis, quantum information theory and quantum cryptology.

by Symantec before the meeting. Also the upcoming TLS 1.3 standard deprecated SHA-1 due to the results of this team's work. Mozilla, Google and Microsoft also adopted their planning regarding SHA-1.
"Although this is not yet a full attack, the current attack is not the usual minor dent in a security algorithm, making it more vulnerable in the far future," adds Ronald Cramer, head of CWI's Cryptology group. Marc Stevens: "As SHA-1 underpins more than 28 percent of existing digital certificates, the results of real-world forgeries could be catastrophic. We hope the industry has learned from the events with SHA-1's predecessor MD5 and in this case will retract SHA-1 before examples of signature forgeries appear in the near future."
This research was partially funded by the Netherlands Organisation for Scientific Research Veni Grant 2014 for Marc Stevens, the Direction Générale de l'Armement, and the Singapore National Research Foundation Fellowships 2012. The results will be shown during the Eurocrypt 2016 conference.

Facts & figures
Output

Papers	295
Books	3
Book chapters	8
Media appearances	178
Software	9
PhD theses	12



Organogram

per 31 December 2015

Governing Board

Peter van Laarhoven, Schiphol Group, chairman
Anton Franken, HU University of Applied Sciences Utrecht
Lorike Hagdorn, TNO
Frank den Hollander, Leiden University
John Koster, ASML
Rineke Verbrugge, University of Groningen

NWO
Netherlands Organisation for Scientific Research

General Director

Jos Baeten

Scientific Advisory Committee

Management Team

Dick Broekhuis
Lynda Hardman
Han La Poutré
Kees Oosterlee

Research Groups

Algorithms & Complexity	**A&C**	Harry Buhrman
Cryptology	**CR**	Ronald Cramer
Database Architectures	**DA**	Stefan Manegold
Distributed & Interactive Systems	**DIS**	Pablo Cesar
Formal Methods	**FM**	Frank de Boer
Information Access	**IA**	Jacco van Ossenbruggen
Intelligent Systems	**IS**	Eric Pauwels
Life Sciences	**LS**	Gunnar Klau
Multiscale Dynamics	**MD**	Ute Ebert
Networks & Optimization	**N&O**	Monique Laurent
Scientific Computing	**SC**	Daan Crommelin
Software Analysis & Transformation	**SWAT**	Jurgen Vinju
Stochastics	**ST**	Bert Zwart
Computational Imaging	**CI**	Joost Batenburg

Service Departments

Communication
Peter Hildering

Financial Administration
Edwin de Boer

Information & Documentation
Lieke Schultze

IT & Facilities
Niels Nes

Personnel & Organization
Angelique Schilder

Secretariat
Hans Hidskes

Centrum Wiskunde & Informatica (CWI) is the national research institute for mathematics and computer science in the Netherlands. The institute's strategy is to concentrate research on five broad, societally relevant themes: Software, Information, Life Sciences, Logistics and Energy.

Visitors address
Science Park 123
1098 XG Amsterdam
The Netherlands

Postal address
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

Phone +31 (0)20 592 93 33
info@cwi.nl

www.cwi.nl

Design
Kitty Molenaar
Printing
Drukkerij Palteam
Publication date
May 2016

Credits

Alessio Bragadini 15
AMC 5
Benschop, Guido 8, 19
CWI 3, 10-11, 11
Omroep MAX 14
Ralf Brinkhoff and Birgit Mögenburg 13
Melchior d' Hondecoeter, Rijksmuseum 4
Shutterstock 2, 6, 7, 9, 12, 16, 17, 18
Universiteit van Nederland 10

CWI
Centrum Wiskunde & Informatica

Contents