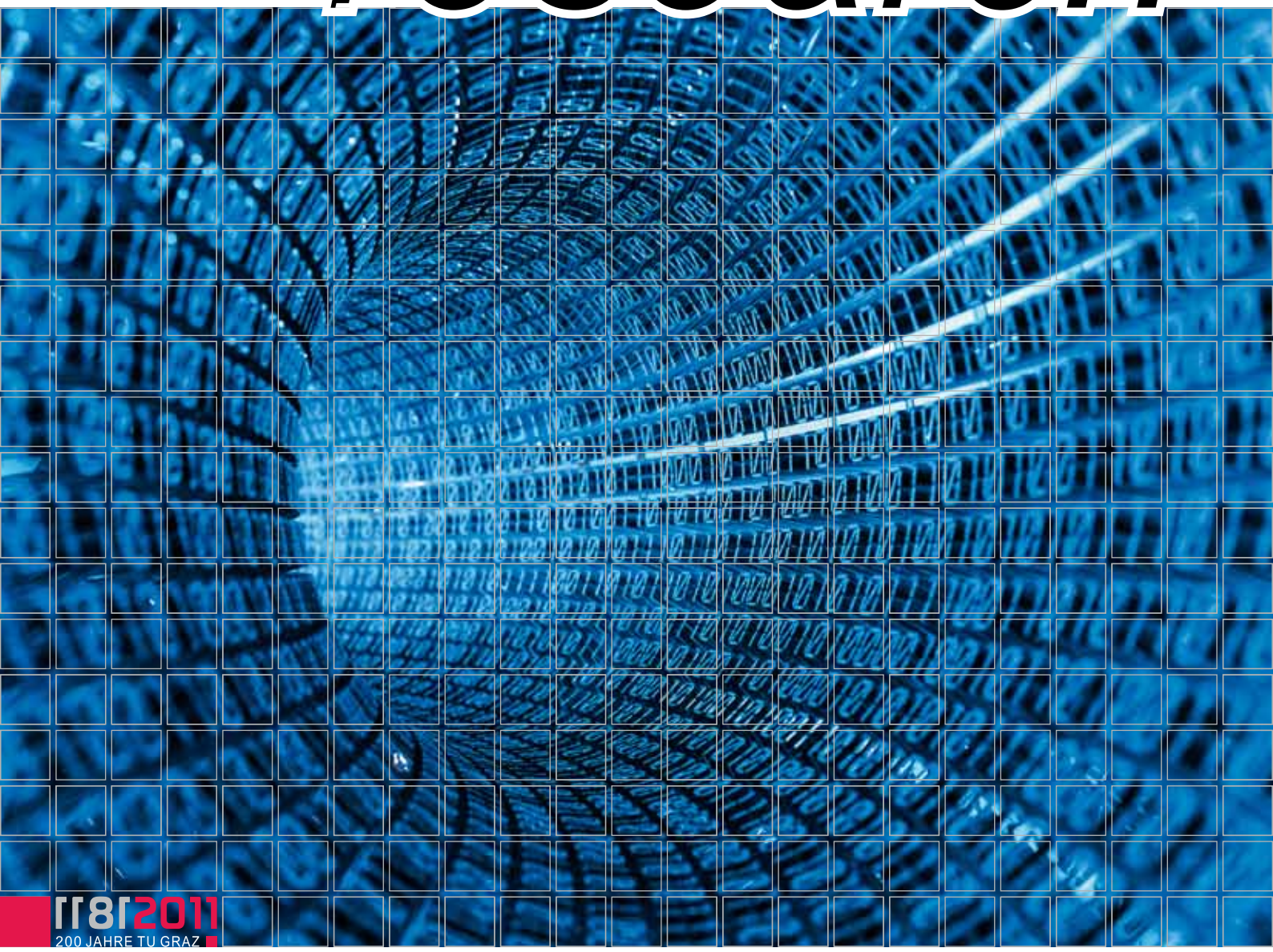
Forschungsjournal der TU Graz

WISSEN ▪ TECHNIK ▪ LEIDENSCHAFT

TU Graz

2011-1 | Nr. 5

TU GRAZ research



1811 2011
200 JAHRE TU GRAZ

Mit Bits und Bytes in die Zukunft

Information, Computing, and Communication Technologies an der TU Graz

Into the Future with Bits and Bytes

Information, Computing, and Communication Technologies
at Graz University of Technology

Content

Inhalt

Liebe Kolleginnen und Kollegen, sehr geehrte Forschungspartner und an unserer Forschung Interessierte!

Dear colleagues, research partners and others interested in our research,

Franz Stelzer, Vizerektor für Forschung und Technologie

Franz Stelzer, Vice President Research & Technology

Entsprechend der Tradition der letzten Ausgaben des TU Graz *research* widmet sich dieses Heft schwerpunktmäßig einem unserer fünf Kompetenzfelder – und zwar dem Field of Expertise Information, Computing, and Communication Technologies.

Dieses Field of Expertise (FoE) hat einen besonderen Stellenwert an der TU Graz. Warum dies so ist, möchte ich Ihnen im Folgenden kurz darlegen: Information, Computing, and Communication Technologies berühren alle anderen Kompetenzbereiche unserer Universität, die „Informatik" spielt heute praktisch in sämtliche Forschungsfelder hinein. Zudem weist dieses FoE die größte Publikationsdichte an der TU Graz auf. Und: Die „Informatik" ist einerseits unsere „jüngste" und personalmäßig kleinste Fakultät, andererseits ist sie die größte, wenn man die zu betreuenden Studierenden berücksichtigt. Wissenschafterinnen und Wissenschafter dieses Kompetenzfeldes nehmen Spitzenpositionen in der europäischen Forschung ein. Besonders erfreulich: Im FoE Information, Computing, and Communication Technologies sind zahlreiche vom FWF geförderte Forschungsprogramme angesiedelt. Drittmittel werden sowohl im ausgezeichneten Grundlagenbereich als auch im anwendungsnahen Forschungsbereich lukriert.

Spannende Geschichten und neue Fakten und Erkenntnisse aus der Forschungswelt der TU Graz erwarten Sie im vorliegenden Heft: Von der Entwicklung des ersten österreichischen Satelliten, an der die TU Graz federführend beteiligt ist, über die Auseinandersetzung mit partiellen Differentialgleichungen bis hin zur Analyse von

Following in the tradition of the last issues of TU Graz *research*, this edition is primarily dedicated to one of our fields of expertise: the field of expertise of Information, Computing, and Communication Technologies.

This field of expertise has special importance at Graz University of Technology, the reasons for which I'd like to outline for you briefly. Information, Computing, and Communication Technologies touch on all the other fields of expertise of our university, and computer science plays a role in practically all of our research fields. Furthermore, more papers are published in this FoE than in any other at Graz University of Technology. Also, computer science is the most recent and, with regard to personnel, the smallest faculty. It's also the biggest when you take into account the numbers of students being supervised. Scientists from this field of expertise take up top positions in European research. Another especially pleasing development is that a large number of research programmes funded by the Austrian Science Fund (FWF) have been established in the FoE Information, Computing, and Communication Technologies. Third-party funds are acquired in outstanding basic and applied research.

Exciting stories and new facts and findings from the world of research of Graz University of Technology await you in this issue. Whether the development of the first Austrian satellite where Graz University of Technology is playing a lead role, the discussion of partial differential equations, or the analysis of fast cryp-

effizienten kryptografischen Bausteinen reicht der Bogen. Lassen Sie sich überraschen, oder haben Sie gewusst, dass Programmieren bedeutet, ein Spiel korrekt aufzulösen?

Abschließend möchte ich mich von Ihnen in der Funktion des „Einleitung schreibenden Vizerektors“ herzlich verabschieden, da meine Funktionsperiode mit Ende September enden wird. Für mich war es eine spannende und aufregende Zeit, in der ich sehr viele neue Erkenntnisse und auch Freunde gewinnen konnte. Besonders gefreut haben mich natürlich der Wissensgewinn aus den Forschungsergebnissen unserer Universität und der damit verbundene Kontakt zu Kolleginnen und Kollegen aus allen Fakultäten. Für diesen persönlichen Zugewinn während dieser Zeit möchte ich mich bei allen bedanken, die nicht nur die Aufgabe übernommen haben, für unser TU Graz *research* Beiträge zu verfassen, sondern mit denen ich auch in den unterschiedlichsten Belangen zusammenarbeiten durfte. Diese wertvollen Begegnungen werden mich in der interdisziplinären Zusammenarbeit und auch im privaten Bereich sicherlich noch über lange Zeit weiter begleiten.

Damit wünsche ich Ihnen allen, Freunden, Kollegen und Kolleginnen und Partnern sowie allen Leserinnen und Lesern dieses TU Graz *research* eine interessante und unterhaltsame Lektüre und weiterhin viele kreative Ideen!

Franz Stelzer

tographic primitives, prepare to be surprised. Or did you already know that programming means finding the right solution to a game.

Finally, in the role of vice-president whose job it is to write introductions, I’d like to make my cordial goodbyes since my term of office will come to a close in September. I have found it an exciting and stimulating time, and it has increased both my knowledge and circle of friends. What has given me special pleasure, of course, has been the advances in knowledge from the research conducted at our university and the contact thus gained with colleagues from all faculties. For this personal gain during this time I’d like to thank everybody – not only those who took on the job of writing articles for TU Graz *research*, but also those with whom I have had the honour to work in the most diverse matters. These valuable encounters will definitely continue to accompany me for a long time in the interdisciplinary collaboration and in my private life.

I would therefore like to wish you all, friends, colleagues and partners, as well as the readership of TU Graz *research*, an interesting and entertaining read and many more creative ideas!

Stolz sein auf Technik aus Österreich und das mit Recht!

Proud of Technology from Austria and Justifiably!

Ines Hopfer

Stefan Rohringer studierte Informatik an der TU Wien und war bis 1999 als Dienststellenleiter im Bereich ASIC Design Center mit Schwerpunkt Design Automation bei Siemens AG, Wien, tätig. 1999 Wechsel zu Infineon Technologies Austria AG, Leiter des Development Centers Graz.

Stefan Rohringer studied computer science at Vienna University of Technology and was department head at ASIC Design Center with focus on design automation at Siemens AG, Vienna. In 1999 he moved to Infineon Technologies Austria AG, as head of the Development Center Graz.

Stefan Rohringer, Leiter des Development Centers Graz von Infineon Austria, plädiert im Interview mit TU Graz research für mehr Zutrauen in technische Errungenschaften und Leistungen „made in Austria“. In Österreich wird Spitzenforschung betrieben, so der Informatiker, doch innerhalb der Gesellschaft werden die Leistungen der Forschenden und Entwicklerinnen und Entwickler kaum beachtet. Eine andere Haltung zur Technik sei notwendig, so Rohringer, um sich den Herausforderungen von morgen stellen zu können.

Sehr geehrter Herr Rohringer, Sie sind der Leiter des Development Centers Graz von Infineon Austria. Infineon Technologies ist weltweit führender Anbieter von Halbleiter- und Systemlösungen für die Themen Automobil, Industrie, Energie und Sicherheit. Wo liegt der Fokus im Development Center Graz?

In Graz legen wir unsere Schwerpunkte auf kontaktlose Sicherheit und auf den Bereich Automobil. Das Development Center (DC) Graz ist ein weltweites Kompetenzzentrum für kontaktlose Technologie in Anwendungen wie Chipcard oder Security ICs, RFID-Lösungen und Funkkomponenten für Anwendungen im Fahrzeug. Ein weiterer Fokus liegt auf dem Antriebsstrang: die Lichtmaschine, ein ganz zentraler Bauteil des Autos. Daneben existiert in Graz noch eine Vorfeldgruppe, die sich mit Fragen von übermorgen beschäftigt.

Infineon Technologies Austria gilt als eines der forschungsintensivsten Unternehmen in Österreich. Wie viel investieren Sie jährlich in Forschungs- und Entwicklungs- und Innovationsprojekte?

Wir haben in Österreich im abgelaufenen Geschäftsjahr (Oktober 2009 bis September 2010) ca. 15 Prozent unseres Österreich-Umsatzes in F&E investiert. Das sind in absoluten Zahlen 200

In interview with TU Graz research, Stefan Rohringer, head of the Development Center Graz at Infineon Austria, makes a plea for more confidence in „made in Austria“ technological achievements. As the computer scientist says, top research is carried out in Austria, but in Austrian society, the achievements of researchers and developers go largely unnoticed. According to Rohringer, a different attitude to technology is necessary in order to be able to meet the challenges of tomorrow.

Mr Rohringer, you’re the head of the Development Center Graz of Infineon Austria. Infineon Technologies is a leading global provider of semiconductor and system solutions in the fields of automotive engineering, industry, energy and security. What does the Development Center Graz focus on?

In Graz our emphasis is on contactless security and the field of automotive engineering. The Development Center (DC) Graz is a worldwide competence centre for contactless technology in applications such as chip cards and security ICs, RFID solutions and radio components for applications in cars. We also have a special focus on powertrains, and in particular alternators – a fundamental component of cars. Parallel to this there is a think tank in Graz, which deals with future questions.

Infineon Technologies Austria is regarded as one of the most research-intensive companies in Austria. How much do you invest annually in research and development and innovation projects?

We invested approx. 15 percent of our Austrian turnover in R&D in the last financial year (October 2009 to September 2010) in Austria. In absolute figures, that’s 200 million euros which has been invested in all the locations in Austria.


TU Graz/Tzivanopoulos

Millionen Euro, die über alle Standorte in Österreich investiert werden.

900 Mitarbeiterinnen und Mitarbeiter entwickeln und forschen für Ihr Unternehmen – welche Rolle spielen hierbei TU Graz-Absolventinnen und -Absolventen?

Infineon Austria hat insgesamt ungefähr 48 Prozent Akademiker und Akademikerinnen. Ein großer Teil von ihnen hat sicher an der TU Graz abgeschlossen.

… und in welchen Funktionen sind diese tätig?

Die Absolventen und Absolventinnen sind großteils in der Forschung und Entwicklung tätig. Aber Sie finden Absolventinnen und Absolventen der TU Graz in allen Bereichen: Das geht von Entwicklungs- und Konzeptarbeiten über Projektleitung bis hinein ins Management.

In Ihrem Imagefolder habe ich das Schlagwort „Innovationsfabrik“ gelesen. Was sind die nächsten Innovationsziele im Bereich F&E bei Infineon?

In der „Innofab“ schauen wir uns besonders die Leistungselektronik an. Die Dünnwafer-Technologie ist hier beispielsweise ein großes Thema. Von Dünnwafer spricht man, wenn der Wafer auf unter 200 Mikrometer dünn geschliffen wird. Infineon ist weltweit der einzige Hersteller, der die Technologie beherrscht, Leistungshalbleiter von nur 40 Mikrometer Dicke zu fertigen. Ein weiteres Thema ist der Bereich E-Mobility: Für die flächendeckende Nutzung von Elektrofahrzeugen ist

900 employees conduct research and development for your company. What role do Graz University of Technology graduates play?

48 percent of Infineon Austria’s employees have a university background. A large number of them definitely graduated from Graz University of Technology.

What positions do they occupy?

They work mostly in research and development. But you’ll find TU Graz graduates in all areas, from development and conceptual work to management.

I read the keyword “Innovation Fab” in your image folder. What are Infineon’s next innovation objectives in the field of R&D?

In the “Innovation Fab”, we pay particular attention to power electronics. Thin-wafer technology, for example, is a big subject. By thin wafers we mean wafers which are cut to less than 200 micrometers thick. Infineon is the only manufacturer worldwide which has the technological proficiency to be able to produce power semiconductors of 40 micrometer thickness. Another subject is the field of e-mobility. For the comprehensive use of electric vehicles, it is necessary to have an infrastructure with a sufficient number of battery charging stations. Here, we have to create the conditions for standardised plug connections and communication interfaces for battery charging and making secure payments. Furthermore, we need an “intelligent” power grid for electricity pro-

eine Infrastruktur mit einer ausreichenden Anzahl an Ladestationen erforderlich. Hier müssen wir die Voraussetzungen für standardisierte Steckverbindungen und Kommunikationsschnittstellen für Ladevorgänge und sicheres Bezahlen schaffen. Wir benötigen weiterhin ein „intelligentes" Stromnetz für CO_2-frei erzeugten Strom. Das sogenannte Smart Grid ist in der Lage, zeitlich und räumlich verteilte Angebots- und Bedarfsspitzen auszugleichen. Bei allen Elektrofahrzeugen spielen Mikrochips eine wichtige Rolle, um das elektrische Fahren effizienter zu machen.

Seit vielen Jahren besteht eine produktive Zusammenarbeit zwischen Infineon Austria und der TU Graz. Inwieweit profitiert Ihr Unternehmen durch diese Kooperation?

Die TU Graz ist einerseits ein sehr wichtiger Ausbildungspartner für uns, anderseits ein wichtiger Partner in diversen Förder- und geförderten Forschungsprojekten. Wir sind auch immer wieder eingeladen, bei Evaluierungen und Lehrplänen mitzuwirken. So wurde auch ein Lehrplan für ein individuelles Masterstudium „Microelectronics – Analog Chip Design" am Institut für Elektronik entwickelt. Die TU Graz ist sehr offen für die Sichtweise der Industrie, was ich sehr schätze. Daneben greifen wir gezielt auf die Expertise der TU Graz im Sinne von Auftragsarbeiten zurück.

Sind weitere zukünftige Kooperationen zwischen der TU Graz und Ihrem Unternehmen geplant und wenn ja, in welchen Bereichen?

Es gibt einige laufende Gespräche. Es gibt einen ganz konkreten Anknüpfungspunkt mit dem K-Zentrum „Virtuelles Fahrzeug", da geht es um den Bereich Batterie im weitesten Sinne, wo wir auf die Kompetenz im K-Zentrum und des Chemie-Instituts zurückgreifen. Die Zusammenarbeit zur Erstellung des individuellen Masterstudiums „Microelectronics" habe ich schon genannt. Eben wurde ein neuer Unternehmenslehrgang zu Reinraumtechnik an der TU Graz gestartet, für dessen Ge-

duced without CO_2. The so-called smart grid is in the position to balance out distributed availability and usage peaks as regards place and time. In all electric vehicles, microchips play a big role in making electric driving more efficient.

There has been a productive cooperation between Infineon Austria and Graz University of Technology for many years. To what extent does your company profit from this cooperation?

Graz University of Technology is a very important training partner for us, and also an important partner in various funded research projects. We are also often invited to collaborate in evaluations and curricula. One example of this was the curriculum for the customised master's programme Microelectronics – Analog Chip Design, which was developed at the Institute of Electronics. Graz University of Technology is very open to the perspective of industry, which is something I appreciate very much. Apart from this, we can selectively fall back on the expertise of Graz University of Technology as regards contract work.

Are there any plans for future cooperations between Graz University of Technology and your company, and if so, in which fields?

There are a number of ongoing discussions. There is a concrete point of contact with the "Virtual Vehicle" K-Centre. This regards the field of batteries in the broadest sense, where we make use of the expertise of Virtual Vehicle Competence Center and the Institute of Chemistry. I've already mentioned our cooperation on the customised master's programme in microelectronics. A new company course in cleanroom technology was launched at Graz University of Technology, for which we at Infineon provided know-how and which will definitely produce optimally qualified young professionals for the industry. Furthermore, talks are currently taking place regarding a new course in the field of energy efficiency.

staltung wir von Infineon Know-how eingebracht haben und der sicher bestens qualifizierte Nachwuchskräfte für die Industrie hervorbringen wird. Weiters laufen gerade Gespräche betreffend eines neuen Lehrgangs zum Thema Energieeffizienz.

IKT sind heute essenzielle Bestandteile unseres Lebens: Handy, Internet, Laptop uvm. prägen unser Leben. Welche Herausforderungen sehen Sie für die IKT-Branche in den nächsten Jahren?

Die IKT ist ein wichtiger Wirtschaftsfaktor und ein Garant für Arbeitsplätze. Aber wir werden in Zukunft noch mehr Mitarbeiterinnen und Mitarbeiter für diese Branche brauchen. Wissen Sie, was ganz dringend notwendig ist, um diesen steigenden Bedarf an Personal decken zu können? Wir brauchen in Österreich eine bessere Stimmung für Technik in allen Lebensbereichen. Jeder hat gern das neueste Handy, aber kaum jemand weiß, wie viel davon in Österreich entwickelt wird! Das fehlt einfach, dieses Zutrauen, dass Österreich es kann. Wir müssen ein „Um-Denken" in der Gesellschaft schaffen. Ein Denken zu: Ich möchte ein Teil dieser Technik sein, die uns Komfort und Sicherheit bringt. Technik ist keine Bedrohung für unsere Weiterentwicklung. Natürlich ist mit Fukushima der Technik-Begriff belastet, aber im Endeffekt ist Technik das, was vieles erst ermöglicht, so leben zu können, wie wir es wollen.

Die IKT-Forschung unterliegt einem rasanten und technologischen Wandel – wie beugen Sie vor, wie meistert Ihr Unternehmen dieses Unterfangen?

Wir holen die besten Köpfe in unser Unternehmen und setzen alles daran, diese zu halten. Und wir versuchen, jetzt die Themen zu identifizieren, die wir übermorgen beherrschen müssen. Diese Fragestellungen brauchen einen langen Atem. Viele Probleme werden wir mit Garantie nicht mehr alleine lösen können, sondern nur mit den richtigen Partnern wie beispielsweise mit der TU Graz.

Today, ICT is an essential component of our lives. Mobile phone, internet, laptop and many more gadgets are shaping our lives. What challenges for the ICT branch do you foresee in the next few years?

ICT is an important economic factor and a guarantor of jobs. But we'll need a bigger workforce for this industry in the future. What is urgently necessary to be able to cover this increasing need is a better atmosphere for technology in Austria in all areas of life. Everyone likes the latest mobile phone but very few people are aware of how many are developed in Austria! This is missing – this confidence that Austria can do it. We need to create a change of attitude in society, along the lines of "I would like to be part of this technology which will gives us convenience and security." Technology is not a threat to our further development. Of course, since Fukushima the term 'technology' has negative connotations, but in end effect, technology is the means to allow us to live the way we want to.

ICT research is subject to rapid and technological change. How do you safeguard against it, how does your company cope with this venture?

We get the best minds for our company and we do everything to keep them. And we try to identify the areas now which we'll have to master tomorrow. These areas need staying power. Many problems we cannot guarantee solving alone, but we will be able to with the right partners, for instance, with Graz University of Technology.

Ab ins All mit dem ersten österreichischen Satelliten:

Das Projekt TUGSAT-1/BRITE-Austria

All Systems Go for the First Austrian Satellite:

TUGSAT-1/BRITE-Austria

Otto Koudelka

Otto Koudelka leitet das Institut für Kommunikationsnetze und Satellitenkommunikation. Die Forschungsaktivitäten umfassen funkgestützte Kommunikationssysteme und -netze (Schwerpunkt Satellitenkommunikation) und deren Anwendungen (u. a. in der Sicherheitsforschung), neuartige Modulations- und Fehlersicherungsverfahren, Entwicklung weltraumtauglicher Hardware.

Otto Koudelka heads the Institute of Communication Networks and Satellite Communications. The institute's research activities comprise radio-controlled communication systems and networks (with a focus on satellite communications) and their applications (in safety research, among other fields), novel modulation and error correction methods, and development of hardware suitable for space.

Am Institut für Kommunikationsnetze und Satellitenkommunikation (IKS) der TU Graz wird derzeit der erste österreichische Satellit namens TUGSAT-1 gebaut, der im dritten Quartal 2011 gestartet werden wird. Derzeit finden die abschließenden Qualifikationstests am Institut statt. Das Projekt stellt eine herausfordernde wissenschaftliche und technologische Mission dar. An Bord befindet sich eine Sternenkamera, die die Helligkeitsschwankungen massiver, heller Sterne (in der Helligkeitsklasse +3.5) mithilfe differentieller Photometrie misst; daher der Missionsname BRITE (Bright Target Explorer).

Astronomen erwarten durch die Langzeitmessung mithilfe der Sternenkamera neue Aufschlüsse über die Rotation und die inneren Vorgänge und damit eine Verbesserung der Theorien über diese Sterne. Möglich werden diese genauen Messungen durch eine präzise miniaturisierte Dreiachsenstabilisierung des Satelliten.

Der ca. 7 kg „leichte" und nur 20 x 20 x 20 cm kleine Satellit bezieht seine Energie aus Solarzellen. Im Mittel stehen etwa 6 Watt zur Verfügung, daher muss der Verbrauch durch ein effizientes Leistungsmanagement so gering wie möglich gehalten werden. Die Sternenkamera, die mit einer Präzisionsoptik mit sehr geringer Lichtdämpfung ausgestattet ist, verwendet einen hochauflösenden CCD-Sensor. Effiziente digitale Modulations- und Fehlersicherungsverfahren garantieren eine sichere Datenübertragung. Der Satellit sendet im Frequenzbereich 2 GHz mit einer Leistung von 0,5 Watt. Die Datenübertragungsrate beträgt nominell 32 kbit/s, wobei das System auf 256 kbit/s ausgelegt ist. Pro Tag wird typisch ein Datenvolumen von ca. 2000 KByte übermittelt.

Der Satellit wird sich auf einer sonnensynchronen Bahn in einer Höhe von ca. 800 km bewegen, womit sich eine Umlaufzeit von ungefähr 100 Minu-

The first Austrian satellite, TUGSAT-1, has been built at the Institute of Communication Networks and Satellite communications (IKS) of Graz University of Technology, and will be launched in the third quarter of 2011. Currently, the satellite is undergoing final qualification tests at the institute. The project is a challenging scientific and technological mission. On board the spacecraft is a star camera which measures the brightness variations of massive luminous stars (in the class +3.5) using differential photometry, from which the mission derives its name – BRITE (Bright Target Explorer).

Astronomers expect to gain new information about the rotation and inner processes of these stars and hence hope to improve the theories about them by means of long-term measurements of the star camera. The accurate measurements are facilitated by a precise three-axis stabilisation of the satellite.

The satellite, which has a mass of only 7 kg and a size of 20x20x20 cm, obtains its energy from solar cells. On average, about 6 W is available, and for this reason the power consumption has to be kept as low as possible through efficient power management. The star camera is equipped with precision optics of low light attenuation and utilises a high-resolution CCD sensor. Efficient digital modulation and error correction techniques guarantee reliable data transmission. The spacecraft transmits in the 2 GHz band at about 0.5 W of power. The data transmission rate is nominally 32 kbit/s, although the system is dimensioned for 256 kbit/s. A data volume of about 2 MByte per day will be transferred.

The satellite will be placed in a sun-synchronous orbit 800 km above the Earth, resulting in an orbital period of 100 minutes. It will be launched by the Indian PSLV rocket (Polar Services Launch

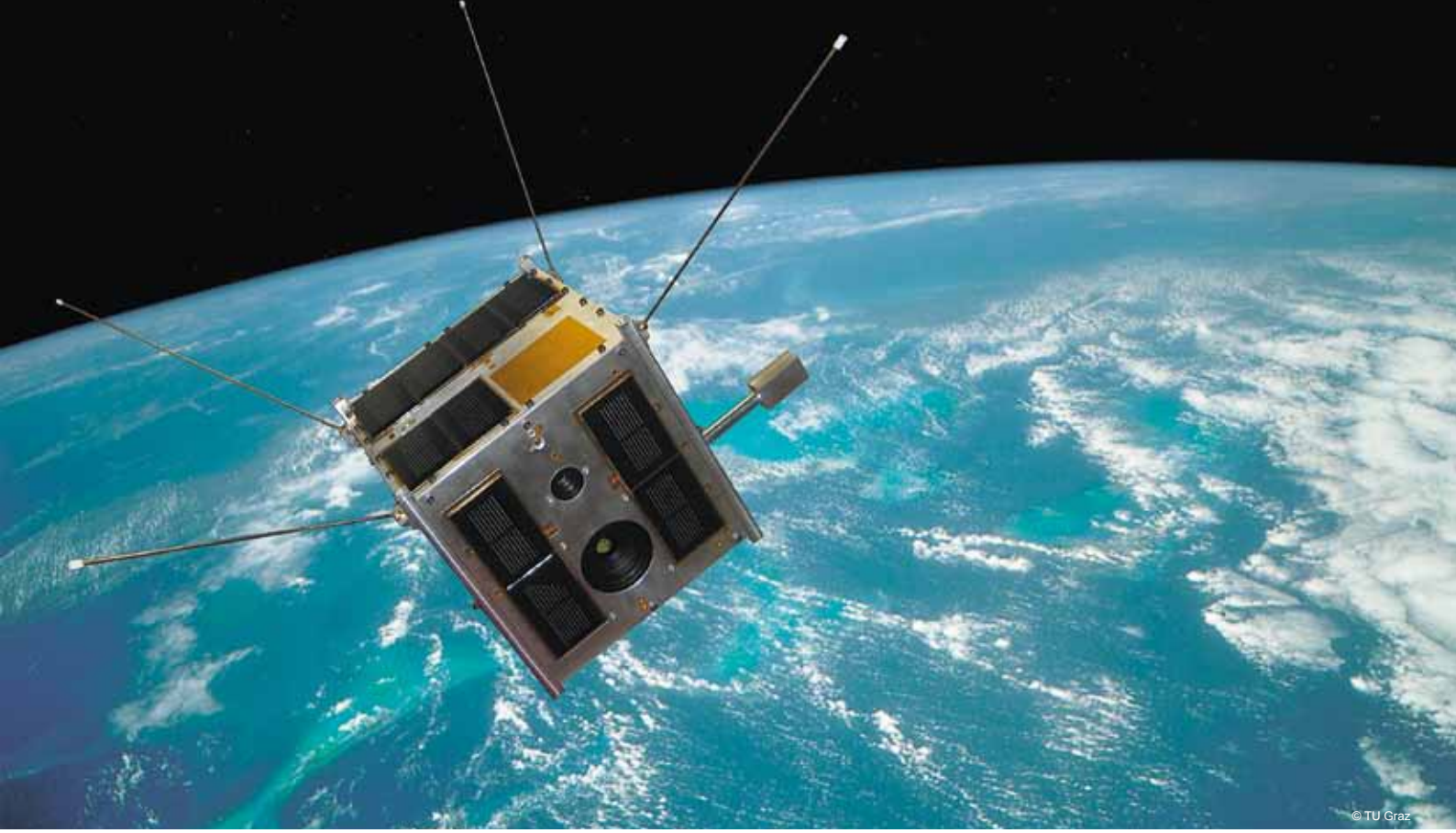


Abb. 1: Modell des Satelliten TUGSAT-1.

Fig. 1: Model of the TUGSAT-1 satellite.

ten ergibt. Gestartet wird mit der indischen PSLV (Polar Services Launch Vehicle)-Rakete vom Satish Dhawan Space Centre in Shriharikota, Indien. Mit derselben Rakete wird der nahezu baugleiche Satellit UniBRITE gestartet, der von der Universität Wien beim Spaceflight Lab der Universität Toronto in Auftrag gegeben worden ist. TUGSAT-1/BRITE-Austria misst die Helligkeitsschwankungen der Sterne im blauen Spektralbereich, UniBRITE im roten. Damit wird eine Konstellation von Nanosatelliten geschaffen, zu der 2012 und 2013 zwei polnische und zwei kanadische Satelliten hinzukommen werden. Durch diese Konstellation werden die Beobachtungszeit und die Menge an wissenschaftlichen Daten deutlich gesteigert.

Am IKS in der Inffeldgasse in Graz wurde das Kontrollzentrum mit einer nachführbaren Antenne mit 3 m Durchmesser für den Satelliten aufgebaut.

Ein wesentlicher Aspekt des Projekts ist die Einbeziehung von Studierenden der drei Universitäten im Rahmen von Diplom-, Projektarbeiten und Dissertationen aus verschiedenen Disziplinen. Damit wird den Studierenden unmittelbare Mitarbeit am Entwurf, Bau, Test und Betrieb des Satelliten, aber auch im Management eines komplexen Weltraumprojekts geboten. Unterstützt werden sie von Weltraumexpertinnen und -experten in Graz und Wien. Bau und Test des Satelliten erfolgen durch Wissenschafterinnen und Wissen-

Vehicle) from the Satish Dhawan Space Centre in Shriharikota, India. The almost identical UniBRITE satellite, ordered by the University of Vienna from the Spaceflight Lab of the University of Toronto, will be launched on the same rocket. TUGSAT-1/BRITE-Austria measures brightness variations in the blue spectral range, while UniBRITE measures variations in the red spectral range. In this way, a constellation of nanosatellites will be created which will be joined in 2012 and 2013 by two Polish and two Canadian satellites. This first nanosatellite constellation will considerably increase the observation time and the amount of scientific data.

The control centre for the satellite with a steerable antenna with a diameter of 3 m has been set up at the Institute in Inffeldgasse, Graz.

One important aspect of the activity is the inclusion of diploma and PhD students in different disciplines in the framework of the projects. Students have the opportunity to cooperate in design, construction, test and operations as well as management of a complex space mission. They are supported by space experts in Graz and Vienna. Implementation and testing is carried out by scientists and technicians of Graz University of Technology.

A dedicated objective is the development of an Austrian nanosatellite platform for future scientific and technological missions, for which considerable interest has been expressed by Austrian space scientists and the space industry.

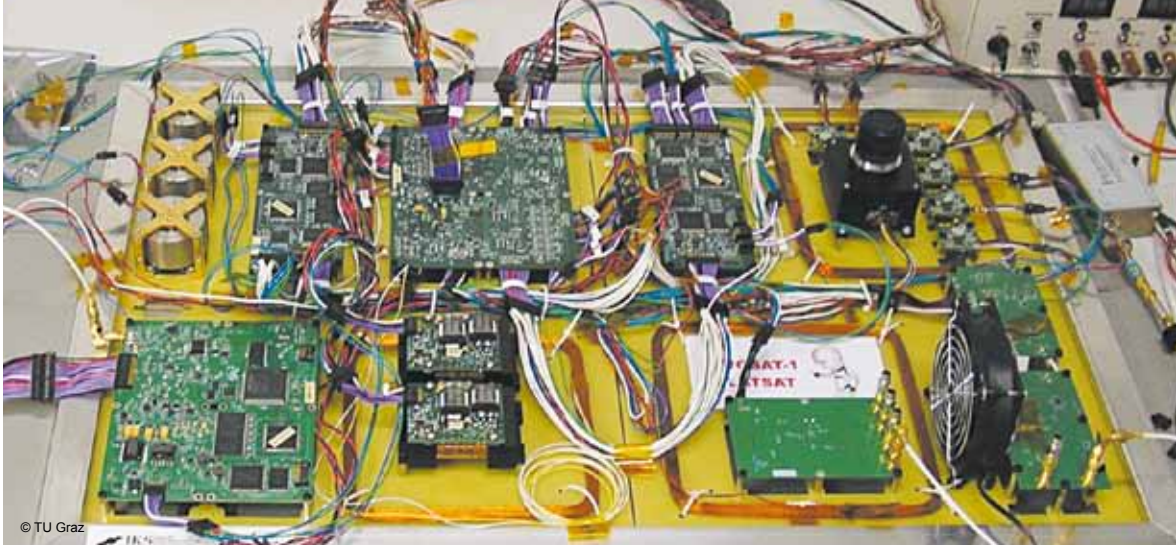


Abb. 2: Test der Subsysteme des Satelliten im Cleanroom des Instituts.

Fig. 2: Testing the subsystems of the satellite in the institute's cleanroom.

Abb. 3: Bodenstation für TUGSAT-1 am Institut für Kommunikationsnetze und Satellitenkommunikation.

Fig. 3: Ground station of the TUGSAT-1 at the Institute of Communication Networks and Satellite Communications.

schafter sowie Technikerinnen und Techniker der TU Graz.

Erklärtes Ziel ist, eine österreichische Nanosatelliten-Plattform für zukünftige wissenschaftliche und technologische Missionen entstehen zu lassen, an der bereits großes Interesse bei österreichischen Weltraumwissenschafterinnen und Weltraumwissenschafter und der heimischen Weltraumindustrie besteht.

Das Projekt wird unter Federführung der TU Graz mit dem Institut für Astronomie der Universität Wien durchgeführt. Die TU Wien ist mit dem Aufbau einer weiteren Bodenstation beteiligt. Enge Kooperation besteht mit dem Spaceflight Lab der Universität Toronto, das beträchtliche Erfahrung im erfolgreichen Bau von Satelliten besitzt. Gefördert wird das Projekt von der Österreichischen Forschungsförderungsgesellschaft FFG im Rahmen des Österreichischen Weltraumprogramms (ÖWP), eines Impulsprogramms des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT).

The project is being carried out under the lead of Graz University of Technology in cooperation with the Institute of Astronomy of the University of Vienna. TU Vienna is also participating with the establishment of an additional ground station. There is close cooperation with the Space Flight Lab of the University of Toronto, which has considerable expertise in successful development of spacecraft. The project is funded by the Austrian Science Promotion Agency in the framework of the Austrian Aeronautics and Space Programme, an impulse programme of the Ministry of Transport, Innovation and Technology (BMVIT).

Funkbasierte Innenraum-Lokalisierungssysteme

Wireless Indoor Localization Systems

Klaus Witrisal, Paul Meissner, Daniel Arnitz

Sei es im Straßenverkehr oder in der Freizeit, zum Beispiel beim Wandern: Wir sind daran gewöhnt, überall verlässlich unsere Position bestimmen zu können. Sobald man aber ein Gebäude betritt, so ändert sich die Situation, vor allem, weil Satellitensignale nicht länger empfangen werden können. Die Liste der möglichen Anwendungsszenarien, die genaue Innenraum-Lokalisierung benötigen, ist jedoch lang: Großeinsätze von Rettungskräften, Verfolgung von Waren in der Logistik oder Leiten von Besuchern und Besucherinnen durch Museen sind nur ein Auszug davon.

Wer sich diese Szenarien genauer ansieht, stellt fest, dass es hier noch immer keine generelle technische Lösung gibt. Nicht zuletzt aufgrund der verschiedenen Anforderungen der genannten Einsatzbereiche kommen völlig unterschiedliche Sensortechnologien wie etwa Laser, Kameras oder Ultraschall zum Einsatz. Mittels dieser Sensoren kann beispielsweise die Distanz zu mehreren bekannten Basisstationen gemessen werden, woraus ein mobiles Gerät seine Position berechnen kann. Die Wireless-Communications-Gruppe des Instituts für Signalverarbeitung und Sprachkommunikation (SPSC) an der TU Graz konzentriert sich auf die Verwendung von Funksignalen zur Lokalisierung, welche einige wichtige Vorteile bieten: Funksignale können prinzipiell Wände durchdringen, über größere Distanzen übertragen werden und Sender und Empfänger können billig gebaut und stromsparend betrieben werden.

Gegenüber diesen Vorteilen ist es aber vor allem die Mehrwegeausbreitung, welche funkbasierten Lokalisierungssystemen zu schaffen macht. Ein am Sender generiertes Signal wird an Wänden und anderen Hindernissen reflektiert und erreicht den Empfänger mehrfach. Diese Reflexionen

Whether in traffic or leisure activities – for instance when hiking – we have become used to being able to reliably determine our position at any time. But the situation changes as soon as we enter a building because satellite signals are no longer available. There is, however, a long list of applications that would benefit from accurate indoor positioning. Large-scale emergency operations, tracking goods in logistics, or guiding visitors in museums are just a few examples.

Looking at these scenarios, it becomes apparent that no generic technical solution exists so far. A variety of sensor technologies have been applied, such as laser sensors, cameras and ultrasound, which reflect the diversity of requirements that various applications have. Using those sensors, distances – for instance – can be measured to a set of fixed base stations in such a way that locations can be computed by a mobile node. The Wireless Communications group of the Signal Processing and Speech Communication Lab (SPSC) concentrates on using radio signals for indoor localization. This approach has important advantages. Objects such as walls can be penetrated in principle, large volumes can be covered, and low-power, low-cost transceivers built.

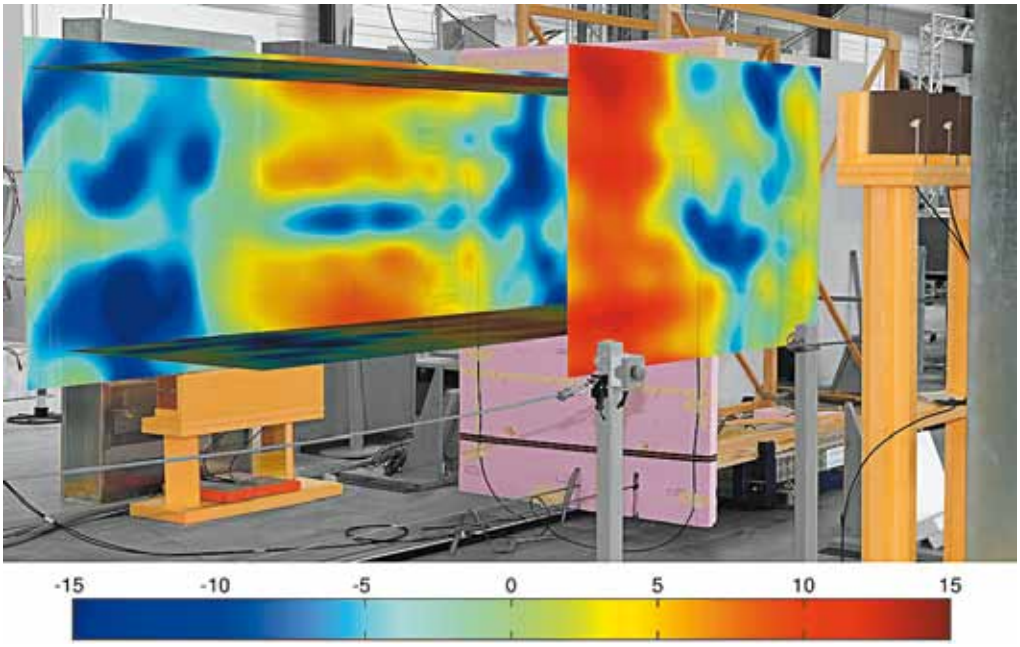
Unfortunately, multipath signal propagation severely hinders the application of wireless indoor positioning systems. A transmitted signal is reflected from walls and other obstacles and hence reaches the receiver through multiple signal paths. This is the main reason for the lack of robustness often encountered. Using the example of Radio Frequency Identification (RFID), our group recently showed that most of the currently proposed methods are based on overly optimistic assumptions regarding the propagation characteristics of the application environment. Detailed

Klaus Witrisal ist Associate Professor am Institut für Signalverarbeitung und Sprachkommunikation und leitet das Arbeitsgebiet Drahtlose Kommunikationstechnik. Seine Forschungsschwerpunkte liegen bei Ultra-Breitbandsystemen zur Datenübertragung und Innenraum-Lokalisierung.

Klaus Witrisal is an associate professor at the Institute of Signal Processing and Speech Communication. He leads the Wireless Communications group, whose research focus is on ultra-wideband systems for communications and indoor localization.

Abb. 1/Fig. 1

© Arnitz



Paul Meissner ist Universitätsassistent am Institut für Signalverarbeitung und Sprachkommunikation und untersucht im Rahmen seiner Dissertation, inwieweit Signalreflexionen und Gebäudepläne für die Lokalisierung verwendet werden können.

Paul Meissner is a research and teaching associate at the Institute of Signal Processing and Speech Communication. His Ph.D. research involves investigating whether signal reflections and building plans can aid radio signal-based indoor positioning systems.

Abb. 1: Kanalmessung in einem RFID-Gate. Das Messergebnis zeigt die unregelmäßige Feldverteilung, die durch die Überlagerung der Mehrwegekomponenten entsteht.

Fig. 1: Channel measurements in an RFID gate. Measurements indicate the randomly distributed, received signal strengths resulting from the superposition of multipath components.

sind der Hauptgrund für die oftmals mangelnde Robustheit dieser Systeme. Am Applikationsbeispiel Radio Frequency Identification (RFID) wurde von uns vor Kurzem gezeigt, dass ein Großteil der vorgeschlagenen Verfahren zur Lokalisierung in diesem Bereich auf zu optimistischen Annahmen beruht. Anhand detaillierter Kanalmessungen und komplexer Simulationen wurden in Zusammenarbeit mit NXP in Gratkorn realistische Anwendungsszenarien evaluiert. Dabei wurde gezeigt, dass die Mehrwegeausbreitung in typischen Aufbauten so massiv ist, dass eine robuste Lokalisierung innerhalb der Parameter von RFID nicht möglich ist.

Bei schmalbandigen Systemen wie eben RFID kann ein Empfänger nur die Überlagerung vieler Reflexionen beobachten. Erst durch Erhöhung der verwendeten Signalbandbreite, was beispielsweise durch das Aussenden immer kürzerer Pulse erreicht werden kann, lassen sich die reflektierten Signalpfade voneinander trennen. In Ultra-Breitbandsystemen, die ein Schwerpunktgebiet unserer Gruppe darstellen, werden Pulse verwendet, welche nur eine Nanosekunde und weniger lang sind. Dadurch wird theoretisch eine zentimetergenaue Positionsbestimmung möglich. Die nun auflösbaren Signalpfade bereiten aber dennoch Kopfzerbrechen: Ist der direkte Pfad zwischen Basisstation und Empfänger blockiert, so kann eine Reflexion eine höhere Signalstärke aufweisen und irrtümlich als direkter Pfad erkannt werden. Dies führt zu großen Lokalisierungsfehlern. Konventionelle Systeme versuchen, solche Fälle zu erkennen, damit die zugehörigen Mes-

channel measurements and system simulations have been used to evaluate such systems in realistic application scenarios. It has been proven that multipath propagation makes robust indoor localization impossible within the parameters of current RFID systems.

In narrowband systems such as RFID, the receiver can just observe the superposition of many signal reflections. This makes the precise measurement of the propagation delay impossible. Increasing the bandwidth, for example by sending extremely short pulses, makes it possible to separate individual signal components. Ultra-wideband systems, which is a special research focus of our group, use pulses that have a duration of less that a nanosecond, and this theoretically allows positioning at centimeter accuracy. However, the multipath components that can now be resolved still cause trouble. If the direct path between the base and mobile nodes is obstructed, reflected signal components can be detected which, in turn, cause large position errors. Conventional systems try to detect and discard such erroneous measurements.

A novel approach developed by our group exploits reflected signal components instead. Assuming prior knowledge of the geometry of an indoor environment, for instance if a floor plan is available, we can treat reflected signals as if they were received from virtual, i.e. physically non-existent, base stations. However, the potentially large number of reflecting surfaces and signal scattering from objects makes an assignment of signal reflections to virtual base stations a hard

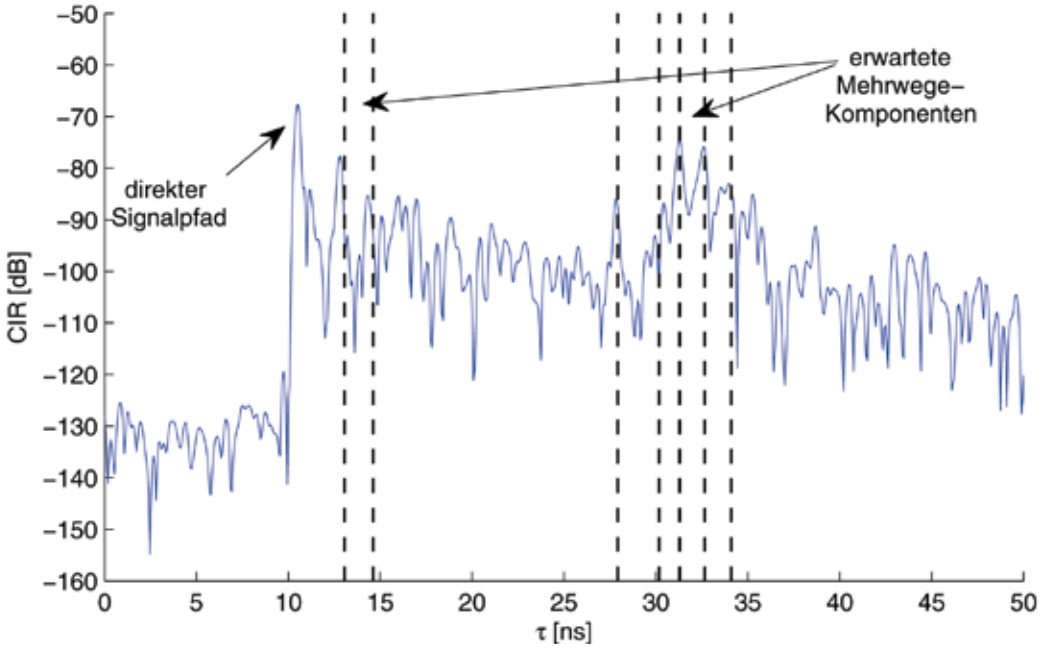


Abb. 2/Fig. 2

© Meissner

sungen verworfen werden und sie die Positionsbestimmung nicht beeinflussen.

Ein von uns entwickelter Lösungsansatz versucht, die reflektierten Signalpfade direkt für die Lokalisierung auszunutzen. Hat man Vorwissen über die Geometrie der Umgebung, zum Beispiel einen Gebäudeplan, so kann man die Reflexionen so verwenden, als wären sie Signale von physikalisch nicht vorhandenen, sogenannten virtuellen Basisstationen. Die Vielzahl an reflektierenden Oberflächen und Effekte wie die Streuung des Signals an Objekten führen aber dazu, dass die empfangenen Signalkomponenten nicht einfach den virtuellen Basisstationen zugeordnet werden können. Um diese Probleme in den Griff zu bekommen, wurde von uns eine Reihe von spezialisierten Tracking-Algorithmen entwickelt. Unsere Ergebnisse zeigen, dass durch geschickte Kombination vorhandener Informationen hohe Robustheit und Genauigkeit im Zentimeterbereich erreicht werden können.

In nächster Zeit werden wir uns im Rahmen unserer Arbeit damit beschäftigen, die von uns entwickelten Verfahren auf ihre Praxistauglichkeit zu überprüfen. Dabei verwenden wir Ergebnisse aus detaillierten Messkampagnen in repräsentativen Umgebungen. Ebenso müssen Lösungen für grundlegende Probleme, wie etwa die geometrische Zuordnung der Reflexionen oder Kooperation mehrerer mobiler Geräte, gefunden werden. Diese Lösungen müssen allgemeingültig sein, damit unsere Verfahren flexibel auf die oben genannten Anwendungen angepasst werden können.

task. Tracking algorithms have been developed to tackle this problem. Our results show that high accuracy and robustness can be achieved by exploiting the available information in smart ways. Looking forward, the methods we have developed will be tested for their suitability in practical situations using measurement data from representative environments. Furthermore, solutions to fundamental problems need to be found, such as the association of signal reflections to geometric features or the cooperation of multiple mobile nodes. These solutions need to be formulated in a generic fashion so that the methods can be flexibly suited to the applications described above.

Daniel Arnitz ist Dissertant am Institut für Signalverarbeitung und Sprachkommunikation und beschäftigt sich mit Verfahren zur Lokalisierung von passiven UHF-RFID-Tags und der Messung und Modellierung von Funkkanälen.

Daniel Arnitz is a Ph.D. student at the Institute of Signal Processing and Speech Communication. He is investigating methods for localizing passive UHF-RFID tags and measuring and modeling of radio channels.

Abb. 2: Impulsantwort eines gemessenen Mobilfunkkanals in einem Innenraumszenario. Markierungen zeigen der Geometrie entsprechende theoretische Ankunftszeiten einiger Mehrwegekomponenten, ebenso sichtbar sind gestreute Komponenten und Messrauschen.

Fig. 2: Impulse response of a measured radio channel in an indoor scenario. Markers show the theoretical arrival times of several multipath components extracted from the geometry of the environment. Also observable are scattered components and measurement noise.

Modellbasiertes Testen (MBT) in der Softwareentwicklung

Model-based Testing (MBT) in Software Engineering

Bernhard Aichernig, Bernhard Peischl, Franz Wotawa

Bernhard Aichernig ist Assistenzprofessor am Institut für Softwaretechnologie (IST) der TU Graz. Seine Forschung konzentriert sich auf die Kombination von formalen Entwicklungsmethoden und fortgeschrittenen Testtechniken. Er war (bzw. ist) leitender Forscher und Projektmanager in drei EU-Projekten zum Thema MBT: CREDO, MOGENTES und MBAT.

▶ http://aichernig.blogspot.com

Bernhard Aichernig is assistant professor at the Institute for Software Technology (IST) at Graz University of Technology. His research focuses on the combination of formal development methods and advanced testing techniques. He has been the key researcher and project manager in three EU projects on MBT: CREDO, MOGENTES and MBAT.

▶ http://aichernig.blogspot.com

Testen zur Sicherung der Softwarequalität hat einen großen Stellenwert. Dies gilt speziell für Systemtests vor Auslieferung der Produkte. Um die Testkosten bei gleicher Qualität zu senken bzw. die Qualität bei gleichen Kosten zu steigern, ist es notwendig, den Systemtest zu automatisieren. Dies kann auf zwei Arten geschehen. Einerseits durch die Automatisierung der Testausführung und andererseits durch die Automatisierung der Testfallgenerierung. Im Artikel werden wir im Speziellen auf die Automatisierung durch die Verwendung von Modellen fokussieren.

Fehler in Programmen sind nicht nur ärgerlich, sondern verursachen der Volkswirtschaft hohe Kosten. Schätzungen gehen hier von direkten und indirekten Kosten in der Höhe von 100 bis 150 Milliarden Euro pro Jahr für Europa aus. Auf Österreich umgelegt sind das 3 bis 4 Milliarden Euro. Neben den volkswirtschaftlichen Kosten haben Programmfehler natürlich auch Auswirkungen auf die Reputation von Firmen. Eine frühzeitige Erkennung und Korrektur der Fehler hat somit einen sehr hohen praktischen Stellenwert. Frühzeitig bedeutet im Umfeld der Softwareentwicklung vor der Auslieferung von Programmen an die Kunden und Kundinnen.

Es gibt eine Reihe von Gründen, die für Fehler in Programmen verantwortlich sind. Zum einen werden Programme noch immer zu wenig getestet. Zum anderen entstehen viele Fehler erst durch das Zusammenspiel von unterschiedlichen Systemteilen beziehungsweise Teilprogrammen. Dieses Problem hat mit der Komplexität der heutigen Programme zu tun, die aufgrund immer höherer Erwartungen an die Funktionalität weiter im Steigen begriffen ist. Um Fehler auf Systemebene zu finden, sind entsprechende Systemtests erforder-

Testing to ensure software quality is of very high importance. This holds especially for system tests performed before software deployment. In order to decrease testing costs while retaining high quality, or increasing quality while keeping testing costs constant, it is important to automate the system test. This can be done either at the test case execution or the test case generation phase. In this article we focus on the automation of test case generation using models of the system under test.

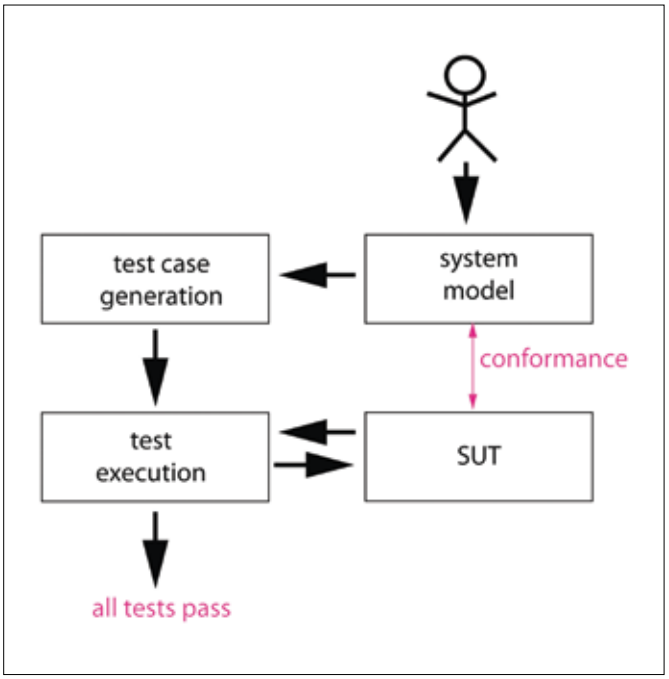
Faults in programs do not only aggravate but also cause costs. Estimates for the direct and indirect costs accrued per annum in the European Union are between 100 and 150 billion euros, which is about 3 to 4 billion euros for Austria alone. Beside the economic costs, there is also the possible loss of reputation of companies developing programs. Therefore, an early detection and correction of faults before program deployment is of great practical interest.

There are a number of reasons why today's programs still fail during use. One reason is the lack of testing during and after development. Another reason lies in the complexity of systems comprising interacting sub-systems where faults are revealed because of the interaction. Unfortunately, the complexity of programs and systems is still increasing because of the increase in demanded functionality. In order to detect faults in interacting systems, a usually rather expensive system test has to be performed.

To reduce the costs of testing while retaining the level of software quality on the one hand and to increase the quality of the software on the other hand, test automation is a must. We distinguish two types of automation – automation of test case execution and automation of test case genera-

Abb. 1: In MBT wird das vom Tester erzeugte Modell zur automatisierten Testfallerzeugung verwendet. Werden alle Testfälle korrekt ausgeführt, dann entspricht das System unter Test (SUT) dem modellierten Verhalten.

Fig. 1: In MBT the tester creates a model, then test cases are automatically generated and executed. If all tests pass, the system under test (SUT) conforms to the model.



lich, die jedoch üblicherweise hohe Kosten verursachen.

Um nun einerseits die Kosten für das Testen zu reduzieren und andererseits die Qualität der Programme zu erhöhen, ist Testautomatisierung erforderlich. Hier unterscheidet man die Automatisierung der Testausführung und die Automatisierung der Testfallerzeugung. Am Institut für Softwaretechnologie beschäftigen wir uns seit mehr als zehn Jahren mit der automatisierten Erzeugung von Testfällen, wobei wir hier die Testfälle aus Systemmodellen gewinnen. Ein Modell beschreibt die gewünschte Funktionalität des Systems. Hier werden unter anderem Automaten (Finite State Machines) oder auch Transitionssysteme (z. B. Labeled Transition Systems) zur Modellierung verwendet, die es ermöglichen, Systemzustandsänderungen abhängig vom aktuellen Zustand und von den Systemeingangswerten zu beschreiben.

Ausgehend von den Modellen können Testfälle erzeugt werden, die gewisse Eigenschaften aufweisen. Im Prinzip funktioniert die Testfallgenerierung durch Analyse des Modells, wobei Sequenzen von möglichen Eingangswerten und erwarteten Ausgangswerten extrahiert werden, die einen Testfall darstellen. Da diese Testfallgenerierungsverfahren auf Modellen basieren, werden sie unter dem Begriff Modellbasiertes Testen (MBT) zusammengefasst (siehe auch Abbildung 1).

In den letzten Jahren wurde am Institut eine Reihe von MBT-Projekten auf EU- (z. B. das FP7-Projekt MOGENTES) und nationaler Ebene (Pro-

tion. The Institute for Software Technology has been working in the area of automating test case generation for more than 10 years. The work is based on system models describing the required functionality of a system. In our case finite state automata and labeled transition systems are used for modeling. This allows for specifying the transition of system states based on the current state and inputs. A test case that is generated automatically from the model is a sequence of inputs and expected outputs. Because of the generation of test cases from models the underlying method is called Model-Based Testing (MBT). Figure 1 illustrates the principle of MBT.

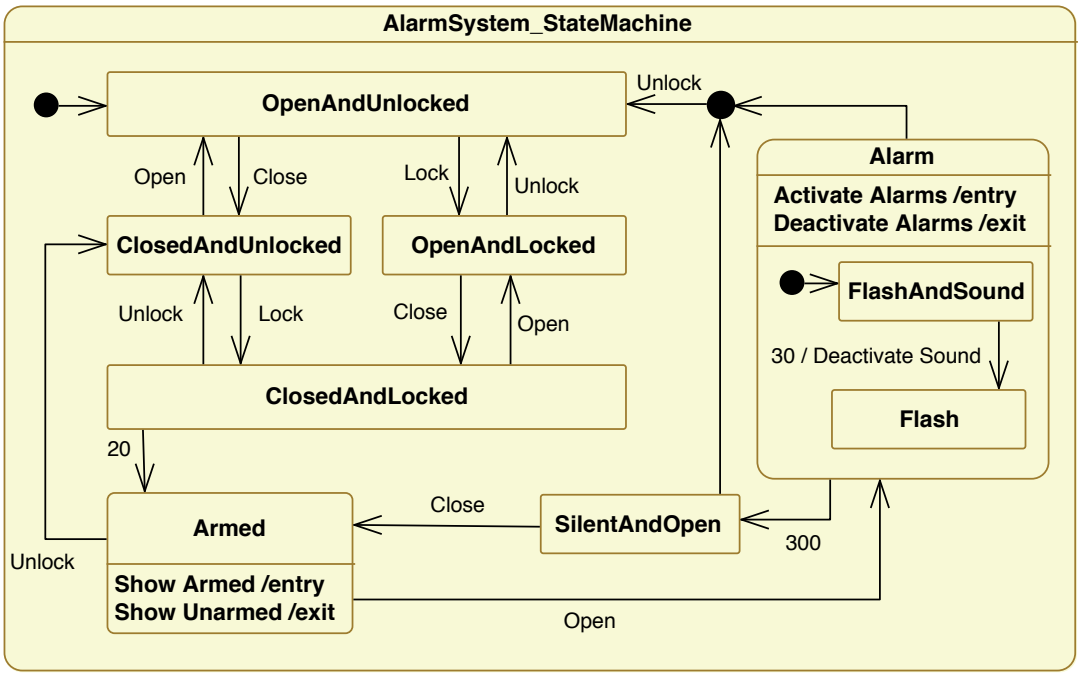
During the past years we have been carrying out several MBT projects, e.g. MOGENTES funded by the European Union, and Softnet funded by the FFG, together with our industrial and scientific partners. The projects have a common focus that lies in transferring basic research results into daily industrial practice, thus leading to new research questions. In particular, providing a well suited modeling language and efficient test-case generation algorithms have been of interest. The efficient generation of tests from highly complex industrial models within a given time has been an especially demanding challenge. In addition, other challenges have been met because of the fruitful collaboration with industry. Generating test cases based on certain coverage criteria for test execution within a limited time, and the prioritization of test case execution are two examples that have been tackled in our projects.

Bernhard Peischl ist Koordinator des Kompetenznetzwerks Softnet Austria (Programme K-net Softnet Austria und COMET K-Projekt Softnet Austria II). Er widmet sich der anwendungsnahen, produktbezogenen Forschung anhand von ausgewählten Referenzprojekten mit Partnern aus der Telekommunikation, dem Automotive-Bereich, der Banken- und Versicherungsbranche sowie Toolherstellern und Beratern.

Bernhard Peischl is the coordinator of the competence network Softnet Austria (Programme K-net Softnet Austria and COMET K-Project Softnet Austria II). He conducts applied and product-specific research by means of selective reference projects with partners from telecommunications, the automotive field and the banking and insurance domain as well as tool developers and consulting companies.

Abb. 2: Ein Modell eines Alarmsystems für Automobile.

Fig. 2: A model of a car alarm system.



Franz Wotawa ist Professor für Softwareentwicklung am Institut für Softwaretechnologie der TU Graz und Leiter des COMET K-Projekts Softnet Austria. Neben dem Modellbasierten Testen forscht er in den Bereichen Automatisiertes Programmdebuggen, Künstliche Intelligenz und Robotik.

Franz Wotawa is full professor at the Institute for Software Technology, Graz University of Technology, and head of the COMET K-Project Softnet Austria. Beside model-based testing, his research focus is on automated program debugging, artificial intelligence, and robotics.

jekte des K-net Softnet Austria und auch Projekte des Nachfolgeprogramms COMET K-Projekt Softnet Austria II) gemeinsam mit Partnern aus der Industrie und Forschung durchgeführt. Gemeinsam ist diesen die Bestrebung, Grundlagenforschungsergebnisse in die industrielle Praxis zu transformieren, was erfahrungsgemäß zu weiteren Forschungsfragen führt. Offene Fragestellungen hierbei waren die Bereitstellung von geeigneten Modellierungssprachen und Testfallgenerierungsalgorithmen. Gerade die Erzeugung geeigneter Testfälle aus komplexen industriellen Modellen war und ist hier eine besondere Herausforderung. Zusätzliche Probleme sind durch industrielle Anforderungen an die erzeugten Testfälle bedingt. So sollen die Testfälle möglichst alle Teile eines Programms ansprechen und auch in einer vorgegebenen Zeit ausgeführt werden können. Eine Priorisierung von Testfällen hinsichtlich gegebener Kriterien wird ebenso angestrebt.

Im Rahmen der MBT-Projekte konnten Lösungen für die meisten dieser Probleme gefunden werden. Unter anderem wurden in einem Projekt Fehler in einer kommerziellen Voice-over-IP (VoIP)-Software gefunden, die durch die vorhergehenden Tests nicht entdeckt wurden. Möglich gemacht wurde dieser Erfolg durch die Modellierung von VoIP-Protokollen und der automatisierten Testfallerzeugung aus diesen Modellen. Nähere Informationen über die Projekte findet man auf folgenden Webseiten:

- www.soft-net.at
- www.mogentes.eu

For most of the open challenges, specific solutions were provided in the projects, and very promising results obtained. For example, with MBT, new faults in a commercial voice-over-IP (VoIP) software have been detected. This was possible due to a model of the VoIP protocol and algorithms for efficiently generating the test cases. More information regarding the projects can be obtained from the project websites:

- www.soft-net.at
- www.mogentes.eu

Partielle Differentialgleichungen – Eine Herausforderung für die moderne Operatortheorie

Partial Differential Equations – A Challenge for Modern Operator Theory

Jussi Behrndt, Jonathan Rohleder

Die mathematische Beschreibung von natur- und ingenieurwissenschaftlichen Vorgängen führt in der Regel zu Gleichungen, in denen Funktionen mehrerer Variablen und deren Ableitungen auftreten. Populäre Beispiele für solche partiellen Differentialgleichungen sind etwa die Schrödinger-Gleichung aus der Quantenmechanik oder die Navier-Stokes-Gleichungen aus der Strömungsdynamik. Da oft nur stark vereinfachte Modellprobleme exakt gelöst werden können, sind qualitative analytische Untersuchungen und numerische Näherungsverfahren für die Praxis unabdingbar. Die moderne Operatortheorie setzt an dieser Schnittstelle mit abstrakten Methoden aus der reinen Mathematik an.

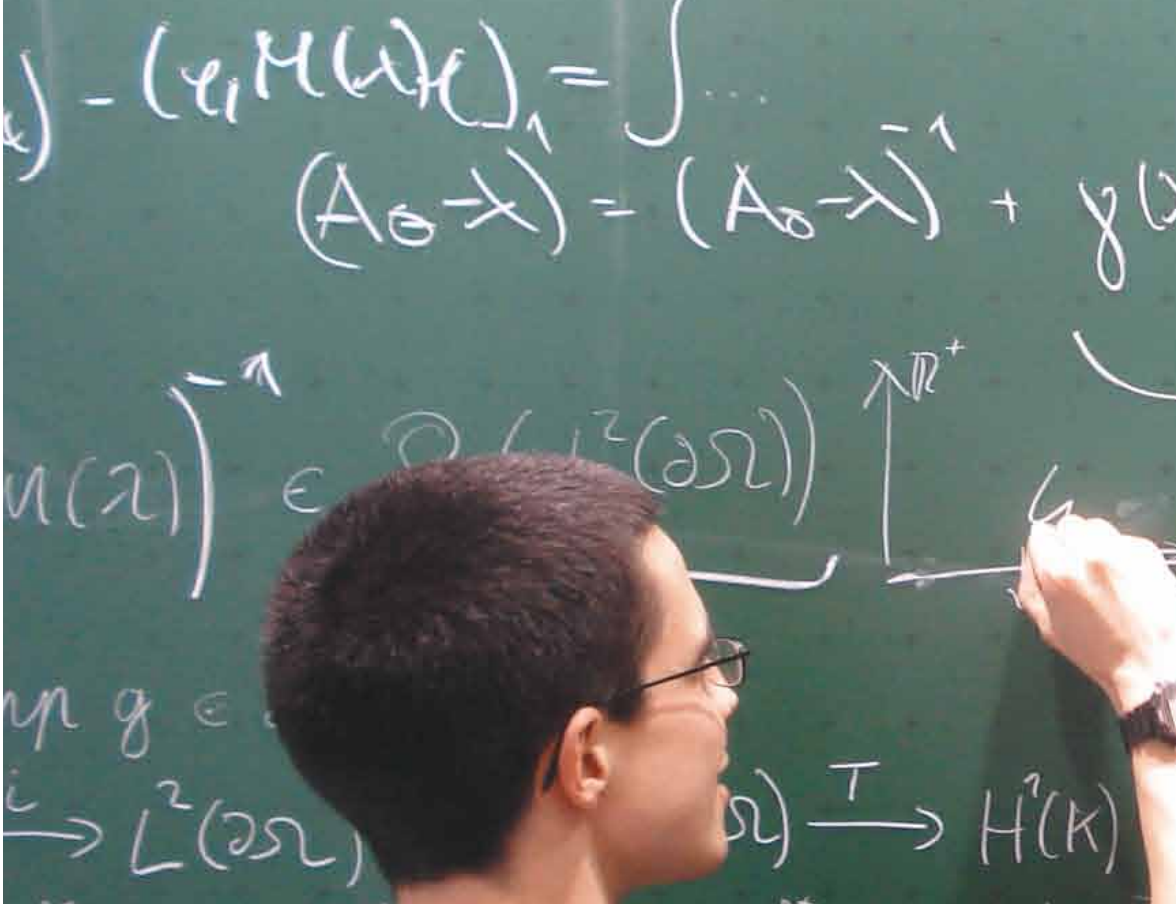
In der analytischen Behandlung von Differentialgleichungen und den zugehörigen Rand- und Anfangswertproblemen stehen die Fragen nach der Existenz, Eindeutigkeit und Stabilität von Lösungen im Vordergrund. Obwohl also für die zugrunde liegenden partiellen Differentialgleichungen keine expliziten Lösungen angegeben werden können, versucht man, strukturelle Aussagen zum Lösungsverhalten zu gewinnen. Funktionalanalytische und operatortheoretische Methoden sind hierbei sehr hilfreich und eröffnen den passenden abstrakten Rahmen für weitergehende Untersuchungen. Beispielsweise ist der Begriff des Spektrums in der Operatortheorie eng verknüpft mit den Spektrallinien von Atomen: Die Eigenwerte und verallgemeinerten Eigenwerte des Schrödinger-Operators beschreiben die möglichen Energiezustände des zugehörigen quantenmechanischen Systems. So lassen sich auch die konzentrischen Bahnen im klassischen Bohr'schen Modell des Wasserstoffatoms gerade als diskrete Energieeigenwerte des entsprechenden Schrödinger-Operators interpretieren.

The mathematical description of processes in natural and engineering sciences typically leads to equations in which functions of several variables and their derivatives appear. Popular examples of such partial differential equations are the Schrödinger equation from quantum mechanics or the Navier-Stokes equations from fluid mechanics. Since in general only very simple model problems are explicitly solvable, qualitative analytic investigations and numerical approximation methods are of great importance in practice. This is where modern operator theory provides the appropriate tools from pure mathematics.

In the analysis of differential equations and the associated boundary and initial value problems, the questions usually focus on existence, uniqueness and stability of solutions. Even though the underlying partial differential equation cannot be solved explicitly, attempts are made to obtain structural properties of the solutions. Functional analytic and operator theoretical methods turn out to be useful here and provide a suitable abstract mathematical framework for further investigations. For example, the notion of the spectrum in operator theory is closely connected to spectral lines of atoms: the eigenvalues and generalized eigenvalues of Schrödinger operators describe the possible energy states of the corresponding quantum mechanical system. Also, the concentric orbits in Bohr's classical model of the hydrogen atom can be interpreted as the discrete eigenvalues of the corresponding Schrödinger operator. One of the main interests of the research group Differential Equations is the spectral theory of partial differential operators. In order to interpret the spectrum under consideration as possible energy states of a quantum mechanical system, the so-called property of selfadjointness of the present problem has to be ensured. Typically this

Jussi Behrndt ist Leiter der Arbeitsgruppe Differentialgleichungen am Institut für Numerische Mathematik. Seine Forschungsinteressen umfassen Spektral- und Störungstheorie, gewöhnliche und partielle Differentialoperatoren, nichtlineare Randwertaufgaben und inverse Probleme.

Jussi Behrndt is head of the group Differential Equations at the Institute of Computational Mathematics. His research interests cover spectral and perturbation theory, ordinary and partial differential operators, nonlinear boundary value problems and inverse problems.



Jonathan Rohleder ist Universitätsassistent in der Arbeitsgruppe Differentialgleichungen. Sein Forschungsgebiet ist die Spektraltheorie von elliptischen Differentialoperatoren.

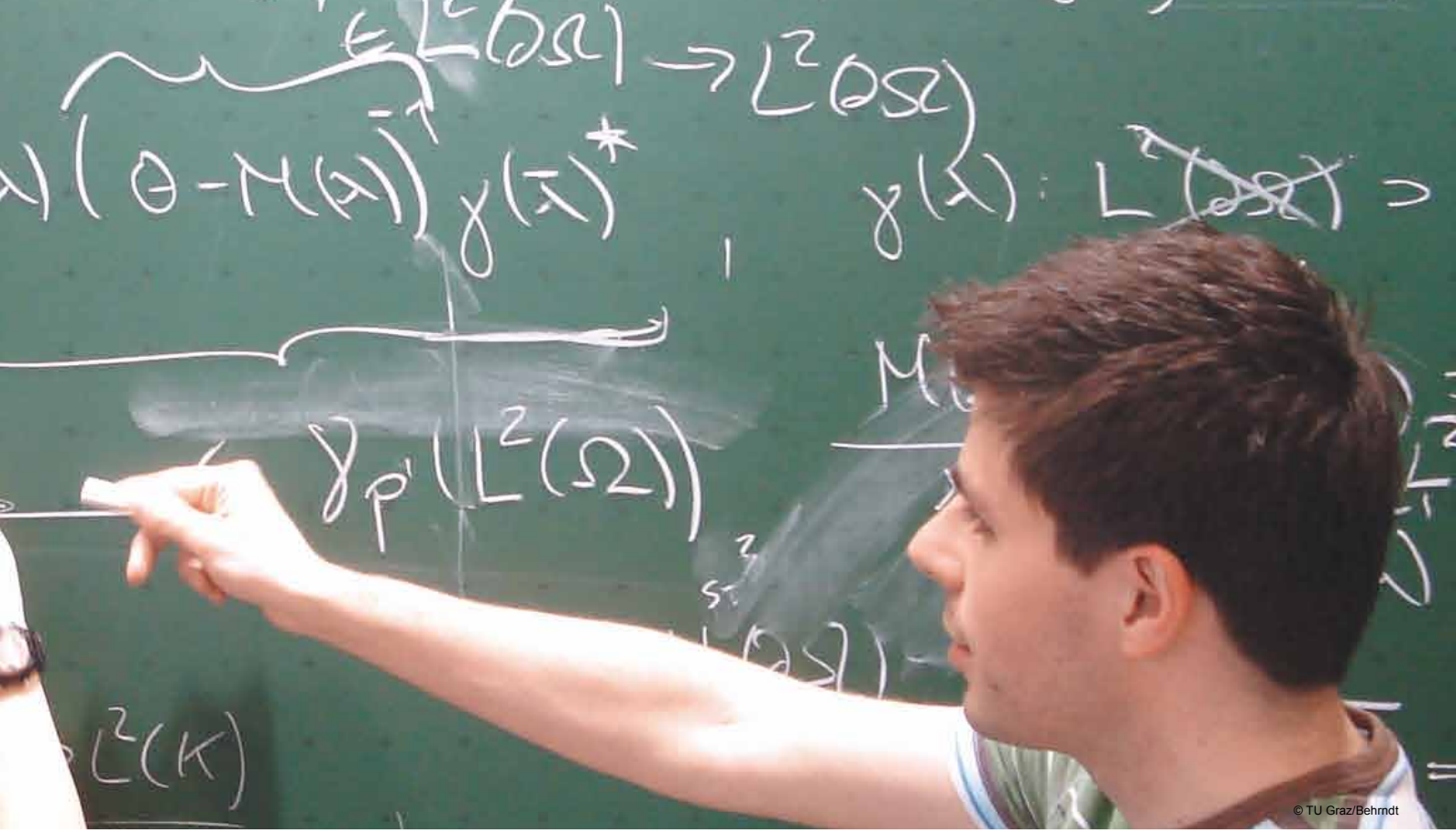
Jonathan Rohleder is research assistant in the group Differential Equations.His field of research is spectral theory of elliptic differential operators.

Einer der Forschungsschwerpunkte in der Arbeitsgruppe Differentialgleichungen ist die Spektraltheorie von partiellen Differentialoperatoren. Um das zu analysierende Spektrum physikalisch sinnvoll als mögliche Energiezustände eines quantenmechanischen Systems interpretieren zu können, ist es besonders wichtig, zuerst die sogenannte Selbstadjungiertheit des betrachteten Problems sicherzustellen. Dies geschieht in der Regel durch eine sinnvolle Wahl von Randbedingungen an das System und kann bei komplizierten Aufgabenstellungen zu einem ausgesprochen anspruchsvollen mathematischen Problem werden. Selbst bei einem einfachen Laplace- oder Schrödinger-Operator auf einem beschränkten Gebiet im zwei- oder dreidimensionalen Raum existiert noch keine adäquate vollständige Beschreibung aller selbstadjungierten Randbedingungen. Die Forscherinnen und Forscher in der Arbeitsgruppe Differentialgleichungen setzen gemeinsam mit ihren internationalen Kooperationspartnern zur Lösung solcher grundlegenden Fragestellungen innovative Techniken und neue Konzepte aus der abstrakten Erweiterungstheorie ein.

Ein weiterer Forschungsschwerpunkt der Arbeitsgruppe ist die analytische Untersuchung verschiedener Klassen von inversen Problemen. Es werden insbesondere verallgemeinerte Varianten des sogenannten Calderón'schen Problems studiert, welches in der elektrischen Impedanztomo-

is done by fixing suitable boundary conditions on the system. However, in complicated settings this may lead to a highly nontrivial mathematical problem. Even for simple Laplace or Schrödinger operators on a bounded domain in two or three space dimensions, a suitable complete description of all selfadjoint boundary conditions does not exist. To solve such fundamental problems, the researchers in the group Differential Equations and their international collaborators apply innovative techniques and new concepts from abstract extension theory.

Another topic which is a central research area of the present group is the analytic investigation of different classes of inverse problems. In particular, generalized variants of the so-called Calderón problem from electrical impedance tomography are studied. The inverse problem in Calderón's classical problem is to determine and reconstruct the conductivity coefficient of an isotropic body by applying a voltage and measuring the corresponding flux on its surface. Under additional regularity assumptions on the surface and the conductivity coefficient, it can be shown that this coefficient is uniquely determined and can be reconstructed by the measured data. The classical Calderón problem was solved about 20 years ago. In the generalized case, where instead of an isotropic body an anisotropic body is considered, fundamental problems arise. The conductivity coefficients are not uniquely determined by voltage



grafie eine wichtige Rolle spielt. Die inverse Aufgabe im klassischen Calderón'schen Problem besteht darin, durch das Anlegen einer Spannung und Messung des resultierenden Stromes an der Oberfläche eines isotropen Körpers den (ortsabhängigen) Leitfähigkeitskoeffizienten zu rekonstruieren. Unter gewissen Regularitätsvoraussetzungen an die Oberfläche und den zu ermittelnden Koeffizienten ist dieser eindeutig durch die Messdaten bestimmt und kann rekonstruiert werden. Das klassische Calderón'sche Problem ist bereits vor 20 Jahren gelöst worden. Für den verallgemeinerten Fall, in dem anstelle eines isotropen Körpers ein anisotroper Körper zugrunde liegt, treten fundamentale Schwierigkeiten auf: Die Leitfähigkeitskoeffizienten sind durch die Messdaten nicht mehr eindeutig bestimmt, d. h., das inverse Problem ist in mathematischer Sprechweise schlecht gestellt. In der Arbeitsgruppe für Differentialgleichungen wird versucht, solche schlecht gestellten inversen Probleme mithilfe von modernen operatortheoretischen Methoden zu kontrollieren. Es konnte beispielsweise gezeigt werden, dass im verallgemeinerten Calderón'schen Problem der zugrunde liegende partielle Differentialoperator bis auf unitäre Äquivalenz aus den Messdaten rekonstruiert werden kann. Besonders bemerkenswert ist, dass hierzu sogar Messdaten auf beliebig kleinen Teilmengen der Oberfläche mit positivem Inhalt ausreichen.

and current measurements on the surface: in mathematical terms, this is a so-called ill-posed inverse problem. Such ill-posed inverse problems are tackled using modern methods from operator theory in the research group Differential Equations. For example, it was proved recently that in the generalized Calderón problem the underlying partial differential operator is determined uniquely up to unitary equivalence and that it can be reconstructed from the boundary measurements. It is a remarkable fact that even measurements on an arbitrarily small subset of the surface with positive volume are sufficient for the uniqueness and reconstruction results to remain valid.

Abb. 1: Forschungsalltag: Mitglieder der Arbeitsgruppe Differentialgleichungen bei der Diskussion neuer Resultate.

Fig. 1: Everday research work: Members of the group Differential Equations are discussing recent results.

Ein mathematischer Zugang zum Design und zur Analyse von effizienten kryptografischen Bausteinen

A Mathematical Approach for Designing and Evaluating Fast Cryptographic Primitives

Vincent Rijmen, Mario Lamberger

Vincent Rijmen arbeitet am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK). Seine Forschungsinteressen sind das Design, die Analyse und die Implementierung von schnellen Algorithmen in der Symmetrischen Kryptografie.

Vincent Rijmen is with the Institute for Information Processing and Communications Technology. He is interested in the design, evaluation and implementation of fast symmetric algorithms.

„Ambient Intelligence", „Internet der Dinge" oder „Smart Dust" sind unterschiedliche Bezeichnungen für ein und dieselbe Entwicklung, nämlich die Verschmelzung von Informationstechnologie mit immer mehr Bereichen unseres täglichen Lebens. Der Übergang zu einem digitalen Alltag bringt ganz neue Herausforderungen. Abgesehen von den bekannten Sicherheitsbedrohungen wie Viren, Phishing und Spam gibt es noch weitere unangenehme Nebenerscheinungen der neuen Technologien.

Ein herkömmlicher RFID-Transponder sendet seine gespeicherte Information an alle in der Nähe befindlichen Lesegeräte aus und kann somit missbraucht werden, um jemanden auszuspionieren. Jede digitale Transaktion hinterlässt Spuren, die in riesigen Datenbanken gespeichert werden, woraus mit statistischen Analysen auf unsere Vorlieben und Verhaltensweisen für Marketingzwecke geschlossen werden kann. Als Gegenmaßnahmen für derartige Bedrohungen stehen uns kryptografische Techniken wie Verschlüsselung, Authentifizierung oder Hash-Funktionen zur Verfügung. Bei der Verschlüsselung gibt es auf der einen Seite Algorithmen wie z. B. RSA, die auf zahlentheoretischen Grundlagen basieren. Diese sichern jedoch in der Praxis nur ca. ein Prozent der eigentlichen Daten. Auf der anderen Seite stehen Algorithmen wie der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES). Diese Algorithmen sind bis zu 10.000-mal schneller als RSA, bauen jedoch auf einem weniger starken mathematischen Fundament auf. Unsere Forschung zielt darauf ab, dieses Fundament zu stärken. Wir wollen das an zwei konkreten Beispielen demonstrieren.

AES

Eine große Gefahr für industrielle kryptografische Applikationen stellen sogenannte „Seitenkanalan-

Ambient Intelligence, the Internet of Things, Smart Dust, ... are different names for the same type of development, namely that digital information processing is entering into more and more aspects of daily life. The transition to the digital economy raises increasing challenges for privacy, security, financial regulation, and intellectual property. Apart from the well-known computer viruses, spam and phishing emails, there are also more subtle threats.

For instance, RFID labels continuously broadcasting data to all listeners, thus allowing people to track all our moves. Every digital transaction leaves traces which are collected in large databases on which data mining techniques are unleashed in order to analyze our daily behavior and our reactions to various marketing techniques, etc.

The only way to counter or moderate these threats is by using cryptographic operations such as encryption, authentication and hashing. While there exist cryptographic operations, e.g. RSA, which are based on strong mathematical foundations, due to their slowness they protect in practice less than one percent of digital data. The vast majority of the data is secured by cryptographic algorithms like the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES), which are up to 10000 times faster than RSA but have a lesser mathematical underpinning. In our research we aim to provide a mathematical framework for the design and evaluation of modern, fast cryptographic operations. Two specific testbeds are being used.

AES

An important threat to commercial cryptographic applications is posed by side-channel attacks, where an attacker measures the electro-magnetic

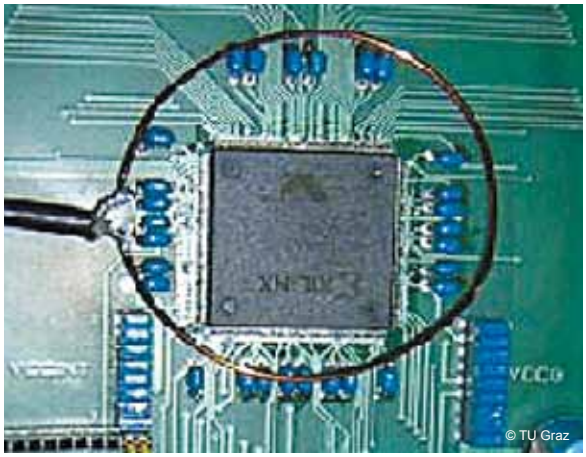


Abb. 1: Messung der elektromagnetischen Abstrahlung bei einer Smartcard mit dem Ziel, den geheimen Schlüssel herauszufinden.

Fig. 1: Electro-magnetic radiation measurement in order to determine the secret key from a smartcard.

griffe“ dar, bei denen ein Angreifer die elektromagnetische Abstrahlung misst, die z. B. eine Smartcard während einer kryptografischen Berechnung verursacht. Der momentane Grad der Abstrahlung steht in engem Zusammenhang mit der durchgeführten Operation und den verarbeiteten Daten. Dies ermöglicht dem Angreifer Rückschlüsse auf den geheimen Schlüssel, der auf diesem Chip gespeichert ist.

Im Rahmen unserer Forschung haben wir mithilfe von „Secret-Sharing“ eine Methode entwickelt, die Seitenkanalattacken vorbeugt. Dabei werden die Daten in drei oder mehrere Teile aufgeteilt, und der Chip arbeitet unabhängig mit diesen „Shares“, aus denen sich jedoch keine Rückschlüsse auf den eigentlichen Schlüssel ziehen lassen. Die Herausforderung bei dieser Methode ist, für eine Verschlüsselungsoperation jene Boole‘schen Funktionen zu finden, die aus den Input-Shares die korrekten Output-Shares berechnen.

Hash-Funktionen

Wann immer ein Dokument digital signiert wird, wird zuerst eine Hash-Funktion auf das Dokument angewandt, um die Daten zu einem digitalen „Fingerabdruck“ zu komprimieren. Aus Performancegründen wird in der Praxis nur dieser Hash-Wert signiert. Ein Sicherheitsproblem in einer Hash-Funktion hat somit gravierende Auswirkungen auf das zugehörige Signaturschema und die daran hängenden Applikationen sowie deren rechtliche Grundlagen (Signaturgesetz, E-Government-Gesetz).

Die US-Behörde NIST (National Institute of Standards and Technology) veranstaltet aktuell einen Wettbewerb mit dem Ziel, den neuen Hash-Standard SHA-3 zu finden. 64 unterschiedliche Designs wurden bis Oktober 2008 als Kandidaten für SHA-3 eingereicht. Ca. ein Drittel dieser Hash-Designs nutzt Teile des AES zur Konstruktion. Dabei konnten wir zeigen, dass ein einfaches blindes

radiation produced by a smartcard during the execution of a cryptographic operation. Because the instant amount of radiation is correlated to the operation being performed and to the logical values that are being processed, it is often possible to determine in this way the secret key used by the chip.

We developed a method based on secret-sharing techniques that counters side-channel attacks. In our method, the sensitive data is never present “in the clear” on the chip. Instead, the data is divided into three or more shares which are all perfectly uncorrelated to the sensitive data and which are processed independently. The consequence is that an attacker may be able to correlate the radiation of the chip to a share, but this doesn’t help to obtain the sensitive data. The research task here is to derive the Boolean functions that are to be applied on the shares of the input in order to obtain the shares of the correct output. Although the mathematical structure of AES facilitates this task, we are still looking for a solution that leads to a good performance at an acceptable cost in hardware.

Hash Functions

Every time a document is signed by means of a digital signature, firstly a hash function is used to compress the document to a “fingerprint.” For performance reasons, the real signature is made on the fingerprint of the document only. Consequently, every new result on the security level of hash functions has a big impact on electronic signature laws and applications, e-government and e-commerce.

The (US) National Institute for Standard and Technology (NIST) is currently running the international SHA-3 competition in order to obtain a new standard hash function. 64 submissions entered the competition in October 2008. Approximately one third of the submissions use (parts of)

Mario Lamberger arbeitet am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK). Sein Forschungsschwerpunkt liegt auf der mathematischen Analyse von Hash-Funktionen und Blockchiffren.

Mario Lamberger is with the Institute for Information Processing and Communications Technology. His interests are the mathematical analysis of symmetric primitives.

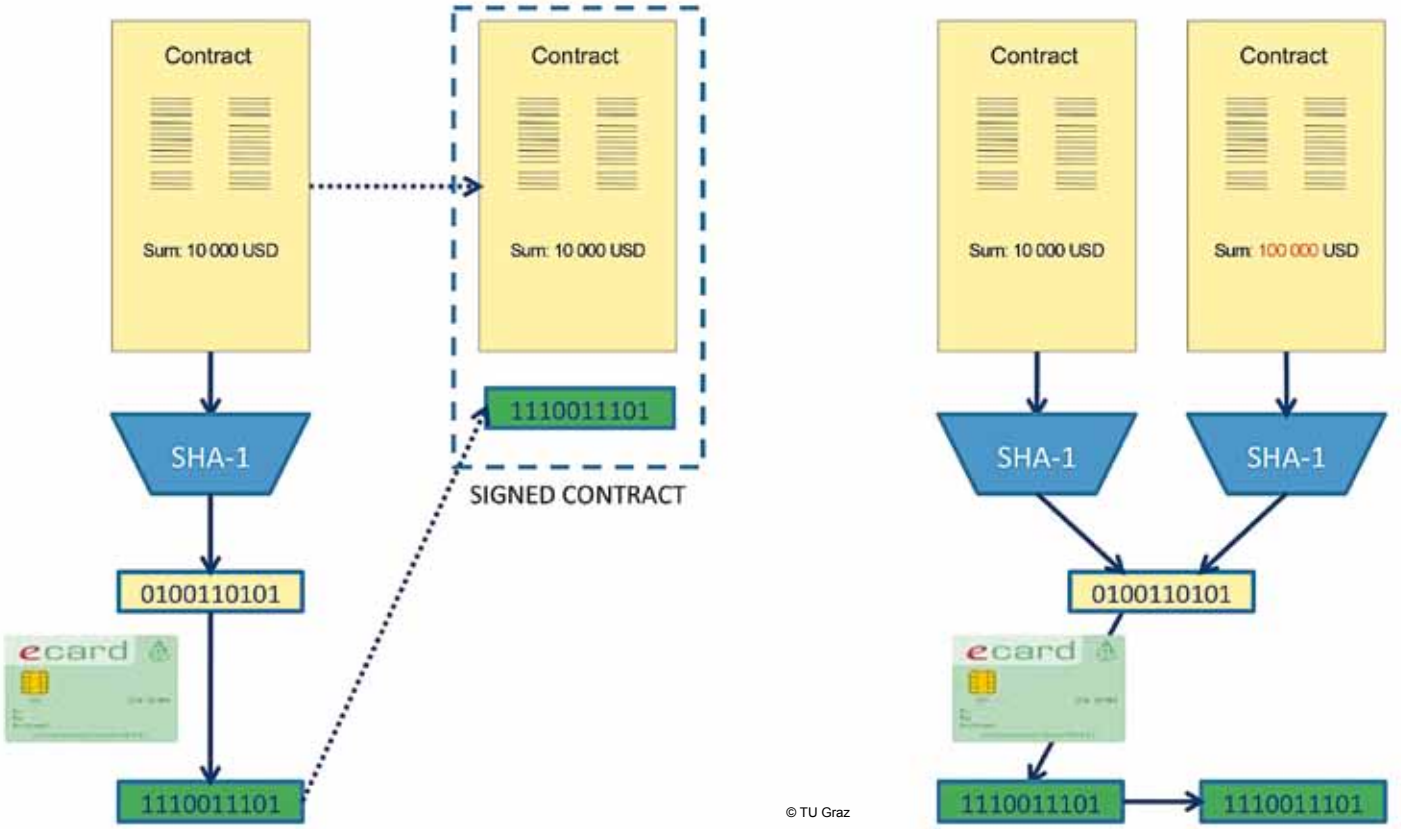


Abb. 2: Der Hash-Wert eines digitalen Vertrags wird eruiert, danach wird die Signatur berechnet (links). Haben zwei Verträge denselben Hash-Wert, sind auch ihre Signaturen gleich: Wenn man einen der Verträge signiert, gilt diese Signatur auch für den anderen (rechts).

Fig. 2: A digital contract is hashed before the digital signature is applied (left). If two different contracts hash to the same value, then their signatures are identical. If you sign one of the contracts, then your signature can be copied onto the other contract (right).

Kopieren der Bausteine des AES zu Sicherheitsproblemen führt. Der bessere Zugang ist es, die gesamte Design-Strategie, die hinter dem AES steht, in Richtung der neuen Anforderungen bei Hash-Funktionen zu adaptieren. Diese Strategie verfolgte das Design-Team der Hash-Funktion „Groestl“, das aus Forscherinnen und Forschern der TU Graz (IAIK) und der Danish Technical University (DTU) besteht. „Groestl“ befindet sich unter den verbleibenden 5 Finalisten im SHA-3-Wettbewerb.

Darüber hinaus haben wir neue mathematische Methoden für die Analyse von Hash-Funktionen entwickelt und diese dazu benutzt, Schwächen in einer Vielzahl von SHA-3-Kandidaten nachzuweisen. Durch den Zusammenhang von gewissen Schwachstellen in einer Hash-Funktion und der Existenz von Code-Wörtern mit geringem Hamming-Gewicht in speziellen linearen Codes wurden automatisierte Tools entwickelt, die die Suche nach diesen Schwachstellen erheblich vereinfachen. Momentan untersuchen wir sogenannte „Covering codes“ auf ihre Anwendbarkeit zur Verbesserung von Attacken auf Hash-Funktionen.

the AES in order to combine security with a high performance. We have shown, however, that blindly copying elements quite often leads to weaknesses. A much better approach is to reuse the AES design strategy and to adapt the components to the new requirements that are posed by the new application. This approach was followed by a joint team of researchers from IAIK and the Danish Technical University (DTU) when they developed the hash function Groestl, which is one of the 5 currently remaining finalists in the SHA-3 competition.

Furthermore, we developed new mathematical methods for the cryptanalysis of hash functions, and used them to break several of the SHA-3 submissions. By linking certain weaknesses in a hash function design to the existence of low-weight code words in a linear code derived from the hash function description, we were able to develop tools that automatically detect this type of weaknesses. Currently, we are exploring the use of covering codes in order to speed up attacks against hash functions.

Know-Center – Österreichs Kompetenzzentrum für Wissensmanagement und Wissenstechnologien

Know-Center – Austria's Competence Center for Knowledge Management and Knowledge Technologies

Michael Granitzer

Suchen Sie stundenlang nach relevanter Information? Passt die gefundene Information nicht zu dem, was Sie bereits wissen? Diese Fragen und mehr lösen Forschungsarbeiten des Know-Center Graz, Österreichs Kompetenzzentrum für Wissensmanagement und Wissenstechnologien. Seit seiner Gründung im Jahr 2001 gestaltet das Know-Center als Bindeglied zwischen Wissenschaft und Wirtschaft die Wissensarbeitsplätze der Zukunft und verbessert damit den Zugang zu Wissen innerhalb von Unternehmen und darüber hinaus.

Die Bewältigung der exponentiell wachsenden Informationsmenge, die uns tagtäglich umgibt, zählt derzeit zu den herausforderndsten Aufgaben im Bereich der Informations- und Kommunikationstechnologien. Während sich Google & Co. um die Anliegen aller „Web-Bewohner und -Bewohnerinnen" kümmern, fokussiert das Know-Center Graz auf das Management von Wissen innerhalb wissensintensiver Organisationen. Im Zentrum stehen dabei Information und deren zielgerichtete Bereitstellung in der tagtäglichen Arbeit. Die am Know-Center in Zusammenarbeit mit Wissenschaft und Wirtschaft entwickelten Technologien gestalten dabei die Wissensarbeitsplätze der Zukunft und tragen als Erfolgsfaktoren zur Zukunft unserer Wissensgesellschaft bei.

Die unseren Technologien zugrunde liegende Forschung richtet ihren Schwerpunkt auf zwei wesentliche Elemente: (i) das Verstehen von Benutzer-Bedürfnissen am Wissensarbeitsplatz und (ii) die semantische Erschließung der für Wissensarbeit benötigten Information. Die Umsetzung dieser Forschungsziele erfolgt dabei in zwei Bereichen am Know-Center: Knowledge Services und Knowledge Relationship Discovery.

Im Bereich Knowledge Services stehen die Kontextualisierung und Personalisierung von Wis-

Do you spend hours trying to find the relevant information? Does the information you find not really fit with what you already know? These questions and more are being solved by research carried out at the Know-Center Graz – Austria's competence center for Knowledge Management and Knowledge Technologies. Since its founding in 2001, the Know-Center has been linking industry and science for designing future knowledge workplaces by improving access to knowledge within the enterprise and beyond.

Coping with the exponential growth of information that surrounds us daily is one of the most challenging tasks in the field of information and communication technologies. While Google & Co. looks after the concerns of all web residents, the Know-Center Graz focuses on the management of knowledge within knowledge-intensive organizations. We thus focus on information and its targeted delivery in day-to-day work. Know-Center's technologies, which are developed jointly with science and industry, design future knowledge workplaces and contribute as success factors to the future of our knowledge society.

The research underlying our technologies focuses on two basic objectives: (i) understanding user needs at knowledge workplaces, and (ii) discovering semantics in information needed for knowledge work. The realization of these research objectives is carried out in two areas at the Know-Center: Knowledge Services und Knowledge Relationship Discovery.

In the area of Knowledge Services, research emphasizes the contextualization and personalization of knowledge services and support for collaboratively creating semantic knowledge structures in organizations. A major challenge here is the automatic identification of user activities, objectives and competencies based on the analysis

Michael Granitzer ist wissenschaftlicher Leiter des COMET-K1-Kompetenzzentrums Know-Center. Entwicklungs- und Forschungsschwerpunkte des Zentrums sind die semantische Erschließung unstrukturierter, heterogener Informationsquellen, visuell gestützte Such- und Analyseverfahren, Recommender-Systeme, emergente Wissensstrukturen sowie informelles und arbeitsintegriertes Lernen.

Michael Granitzer is scientific director of the COMET-K1 competence centre Know-Center. The research and development of the centre focuses on knowledge discovery in unstructured, heterogeneous information sources, visually supported search and analysis methods, recommender systems, emergent knowledge structures, and informal, work-integrated learning.

© Know-Center

Abb. 1: Beispiel-Anwendung mobiles & kollaboratives Mindmapping zur Wissensstrukturierung.

Fig. 1: Example application of mobile & collaborative Mindmapping for knowledge structuring.

sensdiensten und die Unterstützung der gemeinschaftlichen Erstellung von semantischen Wissensstrukturen in Organisationen im Zentrum. Eine große Herausforderung hierbei ist die automatische Identifikation der Nutzeraktivitäten, -ziele und -kompetenzen über die Analyse von Nutzungs- und Sensordaten. Die Einbeziehung dieser Analysen ermöglicht es, die Evolution von Wissensstrukturen zu unterstützen und Wissensarbeiter mittels kontext-sensitiver Recommender-Systeme mit relevanter Information zu versorgen. Hierbei kommen hybride Verfahren, welche die Vorzüge semantischer mit denen probabilistischer Technologien vereinen, und daher auch mit limitierten Datenmengen im Unternehmenskontext effektiv sind, zum Einsatz.

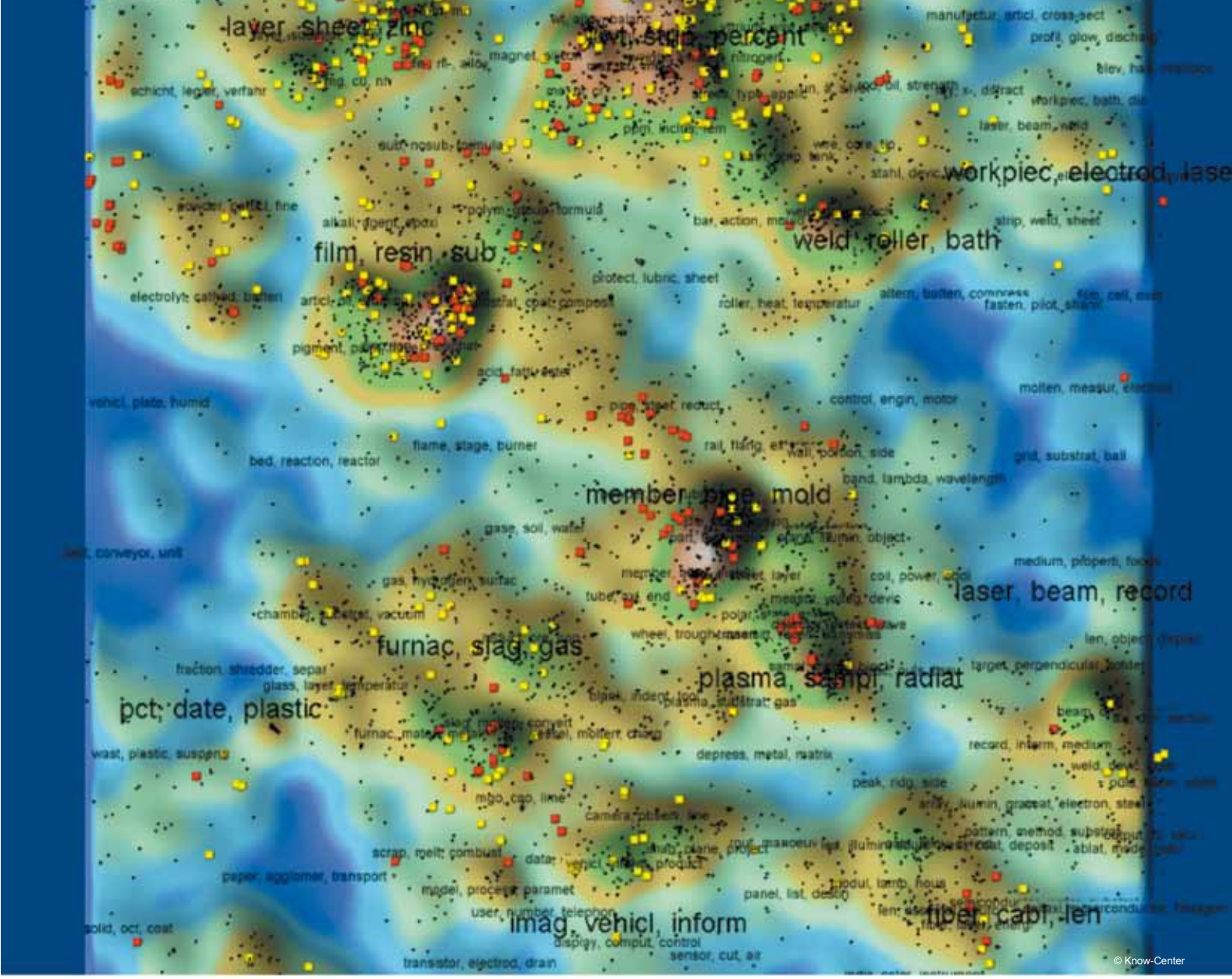
Der zweite Bereich, Knowledge Relationship Discovery, fokussiert auf verteilte, heterogene Information und die Extraktion des darin enthaltenen Wissens. Zu den größten Herausforderungen zählt dabei der Umgang mit einer ständig wachsenden Anzahl umfangreicher, komplexer, dynamischer Informationsquellen. Das zuverlässige Finden relevanter Information wird dadurch zu einem entscheidenden Produktivitäts- und Innovationsfaktor. Fortgeschrittene Erschließungs- und Visualisierungsverfahren sind in der Lage, relevantes Wissen in Informationsquellen automatisch zu identifizieren und direkt am Arbeitsplatz, maßgeschneidert für die aktuelle Aufgabenstellung, zur Verfügung zu stellen. Damit schafft die Wissenserschließung eine wesentliche Voraussetzung für effiziente und erfolgreiche Wissensarbeit.

Die erzielten Forschungsergebnisse führen dabei zu nachhaltigen Innovationen unserer 22 Industriepartner. Kontextsensitive Recommender-Systeme, semantische Suchdienste, webbasierte Open-Innovation-Prozesse und mobile, kollaborative Mindmapping-Lösungen sind nur einige Beispiele, mit denen sich unsere Partner erfolgreich

of usage and sensor data. Taking this analysis into account allows for supporting the evolution of knowledge structures and for providing relevant information to knowledge workers with the help of context-sensitive recommender systems. Such recommender systems combine the benefits of semantic and probabilistic techniques to counteract the limitations of smaller data sets encountered within enterprises.

The second area, Knowledge Relationship Discovery, focuses on the transformation of distributed, heterogeneous information into knowledge that is relevant for users. One of the major challenges in this regard is the constantly growing number of massive, complex and dynamic information sources. Efficient search and reliable retrieval of relevant information has become a decisive productivity and innovation factor in this context. Advanced discovery methods are capable of automatically identifying relevant knowledge in information sources and delivering such knowledge directly to a user's workplace based on current work context. Knowledge relationship discovery therefore provides the foundation for efficient and successful knowledge work.

The results of our research has led to sustainable innovations for our 22 partners in industry. Context-sensitive recommender systems, semantic search services, web-based open innovation processes, and mobile, collaborative mind-mapping solutions are just a few examples through



auf dem Markt platzieren konnten. Davon profitiert auch die TU Graz: Die oben genannte Online-Mindmapping-Lösung steht allen Personen innerhalb der TU Graz in der Premiumversion gratis zur Verfügung[1], und die APA DeFacto stellt Inhalte innerhalb des TU Graz-Netzwerks zur Verfügung[2].
Zur Umsetzung dieses ehrgeizigen Forschungs- und Innovationsprogramms kooperiert das Know-Center mit der TU Graz, JOANNEUM Research, der Karl-Franzens-Universität sowie mit renommierten Forschungsinstitutionen in Europa und Asien. Die internationale Sichtbarkeit zeigt sich auch in unserer seit nunmehr 11 Jahren veranstalteten internationalen „I-KNOW"-Konferenz. Rund 500 Teilnehmende treffen sich jährlich in Graz, um sich über Theorie und Praxis von Wissensmanagement und Wissenstechnologie auszutauschen.

which our partners have achieved success on the market. This is also beneficial for Graz University of Technology. For example, the premium version of the above-mentioned online mind-mapping solution is freely available to all persons at the university. Furthermore, the APA de facto content can also be accessed without charge from within the Graz University of Technology network[2].
To implement this ambitious research and innovation programme, Know-Center Graz cooperates closely with the Graz University of Technology, JOANNEUM Research, Karl-Franzens-University Graz and other renowned research institutions in Europe and Asia. International visibility is also evident in our international "I-KNOW" conference held for the past 11 years. Around 500 participants meet annually in Graz to discuss theory and practice of Knowledge Management and Knowledge Technology.

Abb. 2: Visuelle Analyse von Zusammenhängen in großen, unstrukturierten Dokumentmengen.

Fig. 2: Visual Analysis of relations in large, unstructured document data sets.

[1] *https://tugraz.mindmeister.com/de/team/login*
[2] *http://know-center.tugraz.at/news/2010/01/apa-defacto-campus-fur-tug-studierende-gratis*

Hybrid-Brain-Computer Interface – Ein neues assistierendes Hilfsmittel?

Hybrid Brain-Computer Interface – A New Assistive Device?

Gernot Müller-Putz

Gernot Müller-Putz ist Associate Professor am Institut für Semantische Datenanalyse. Seine Forschungsschwerpunkte liegen bei Brain-Computer-Kommunikationssystemen, Neuroprothesen bei Querschnittgelähmten, dem menschlichen somatosensorischen System und in der assistierenden Technologie.

Gernot Müller-Putz is associate professor at the Institute for Knowledge Discovery. His research interests include brain-computer communication systems, neuroprosthetics in spinal cord injured, the human somatosensory system and assistive technology.

Am Institut für Semantische Datenanalyse werden zurzeit fünf EU-Projekte zum Thema Brain-Computer Interface bearbeitet, ein EU-Projekt wird von der TU Graz koordiniert. Einer der Schwerpunkte ist es, das Brain-Computer Interface (BCI) aus dem Labor in den klinischen Alltag zu bringen. Eine Möglichkeit dafür wird im Folgenden beschrieben.

Personen mit schwersten Beeinträchtigungen steht eine große Auswahl von assistierenden Hilfsmitteln zur Verfügung. Die Liste der Hilfsmittel reicht von einfachen Schaltern oder Tastern, die mit einer Fernsteuerung verbunden sind, über komplexe Sensoren (z. B. Mundmaus), die an einen Computer angeschlossen sind, bis hin zu Eye-Tracking-Systemen. Diese Systeme arbeiten sehr gut, nachdem sie individuell an die jeweilige Person angepasst wurden. Es gibt aber Situationen, in denen diese nicht einwandfrei funktionieren, z. B. wenn eine Ermüdung der noch vorhandenen Muskulatur auftritt, die normalerweise zur Steuerung verwendet wird. In einem solchen Fall stellt das Brain-Computer Interface (BCI) eine gute Option dar, die Steuerung, ohne die Notwendigkeit von Bewegungen, zu übernehmen.

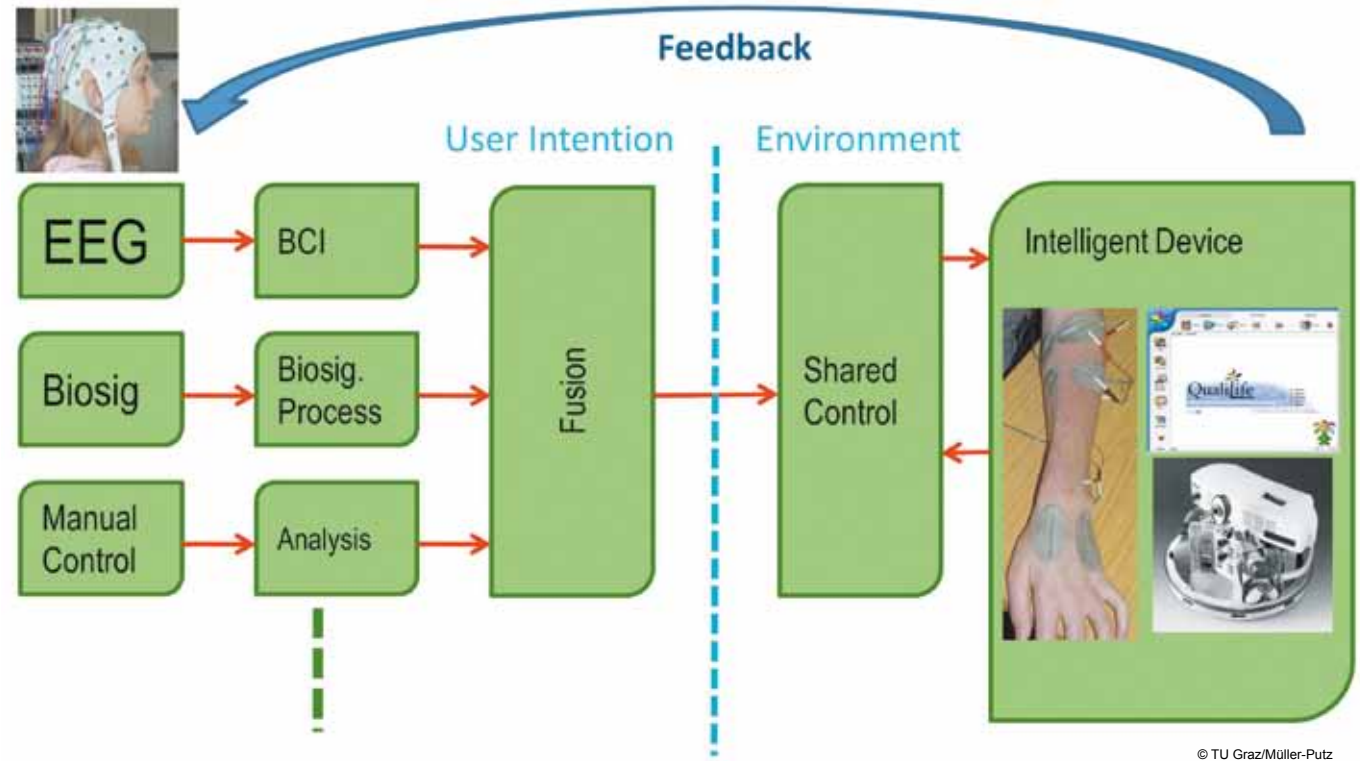
Ein BCI ist ein System, das es einem Benutzer/einer Benutzerin ermöglicht, nur durch Denken, ohne jegliche Muskelbewegung, eine Anwendung zu steuern. Dabei wird die Gehirnaktivität gemessen, daraus wird Information gewonnen und in Steuersignale umgesetzt. Für beeinträchtigte Personen stellt das BCI eine Möglichkeit zur Kommunikation dar. BCIs können auch von Querschnittgelähmten mit hoher Läsionshöhe zur Steuerung von Neuroprothesen zur Griffwiederherstellung verwendet werden. Nach ungefähr 20 Jahren Forschung und Entwicklung ist das Brain-Computer Interface (BCI) eine Technologie, die das Labor verlässt und in die klinische Anwendung kommt. Das BCI könnte als Kommunikationssystem fun-

Currently, five EU projects involving Brain-Computer Interfaces are in progress at the Institute of Knowledge Discovery, one of which is coordinated by Graz University of Technology. One major challenge is bringing Brain-Computer Interfaces (BCI) out of the lab into real-world settings. One possible solution is described below.

Persons with movement disabilities can use a wide range of assistive devices (ADs). The set of ADs ranges from simple switches connected to a remote controller to complex sensors (e.g. mouth mouse) attached to a computer and to eye-tracking systems. All of these systems work very well after being adjusted individually for each person. However, there are still situations where the systems do not work properly, e.g., when residual muscles become fatigued or users have such severe disabilities that no movement is possible. In such situations, a Brain-Computer Interface (BCI) might be the only available option, since they use brain signals (usually the electroencephalogram, EEG) for control without requiring any movement whatsoever.

BCIs are systems that establish a direct connection between the human brain and a computer, thus providing an additional communication channel. As noted, some people use a BCI because their disabilities make it impossible to use any interface requiring movement. BCIs can also be used to control neuroprostheses in patients suffering from a high spinal cord injury, for example by using Functional Electrical Stimulation for grasp restoration. After 20 years of research and development, Brain-Computer Interface technology is ready to leave the lab and to be used in practical applications in real-world settings such as homes or hospitals.

A BCI could replace an existing AD. However, it would be even better to couple the BCI with the existing AD and develop a new system called a hybrid



© TU Graz/Müller-Putz

Abb. 1: Prinzip des Hybrid-BCI.

Fig. 1: Principle of a hybrid BCI.

gieren und das bestehende assistierende Hilfsmittel zeitweilig ersetzen – oder noch besser, das BCI könnte mit den vorhandenen assistierenden Systemen zu einem neuen System gekoppelt werden. Ein solches System, hybrides Brain-Computer Interface (hBCI) genannt, wird derzeit am Institut für Semantische Datenanalyse, TU Graz, im Rahmen des EU-Projekts TOBI (Tools for Brain-Computer Interaction, www.tobiproject.org) erstellt. Bei diesem hBCI ist das BCI immer verfügbar, sobald der Benutzer/die Benutzerin diese Erweiterung des bestehenden Assistsystems wünscht. Es kann aber auch sein, dass das BCI nicht zur Steuerung verwendet wird. Das hBCI entscheidet also einerseits, welche Eingabesignale am zuverlässigsten sind und kann somit die besten auswählen, um die Informationstransferrate und Benutzerfreundlichkeit zu verbessern, andererseits kann es Signale kombinieren, um diese Verbesserungen zu erreichen.

An unserem Institut wurden und werden verschiedene Studien zu diesem Thema durchgeführt, jedoch haben diese gemeinsam, dass entweder ein BCI mit einem BCI (mit verschiedenen Hirnsignalen) oder ein BCI mit einem anderen Biosignal gekoppelt wurde (EU-Projekt BRAINABLE). Das hier vorgestellte hBCI hängt aber nicht alleine von einem BCI ab. Es erlaubt dem BCI, als Eingabekanal zu arbeiten, sobald das BCI die allgemeine Performanz für den Benutzer/die Benutzerin erhöht. Das hBCI kann aber auch eine Fusion von verschiedenen Eingangssignalen vornehmen, um ein einziges Steuersignal zu bekommen, oder es wählt zwischen den vorhandenen Eingangssignalen aus.

BCI (hBCI). Currently, several hBCI systems are under development at the Institute for Knowledge Discovery within the EU project TOBI (Tools for Brain-Computer Interaction, www.tobiproject.org).

Ideally, a hybrid BCI should let the user extend the types of inputs available to an assistive technology, or choose not to use the BCI at all. The hBCI might decide which input channel(s) offers the most reliable signal(s) and switch between input channels to improve information transfer rate, usability, or other factors, or could instead fuse various input channels.

Various studies about hBCIs have been conducted in the past and are being presently conducted, but they all have one thing in common – they combine a BCI with another BCI (using different brain signals) or a BCI with another biosignal (EU Project BRAINABLE). The described hBCI does not depend on the BCI as an input. Instead, it simply allows the BCI to function as an input channel when the BCI could increase the overall performance for that user. The hBCI can perform fusion to switch between multiple inputs, but (depending on the configuration) can also weight signals and combine/fuse them to achieve one control signal from a combination of multiple inputs.

The principle of such an hBCI can be seen in Figure 1. In addition to the EEG-based BCI, other input and control signals are shown. These include other biosignals as well as signals from manual controls such as from ADs (e.g., mouth mouse, push buttons, …). The “fusion” generates a new control signal out of all inputs. Besides a quality check (e.g.,

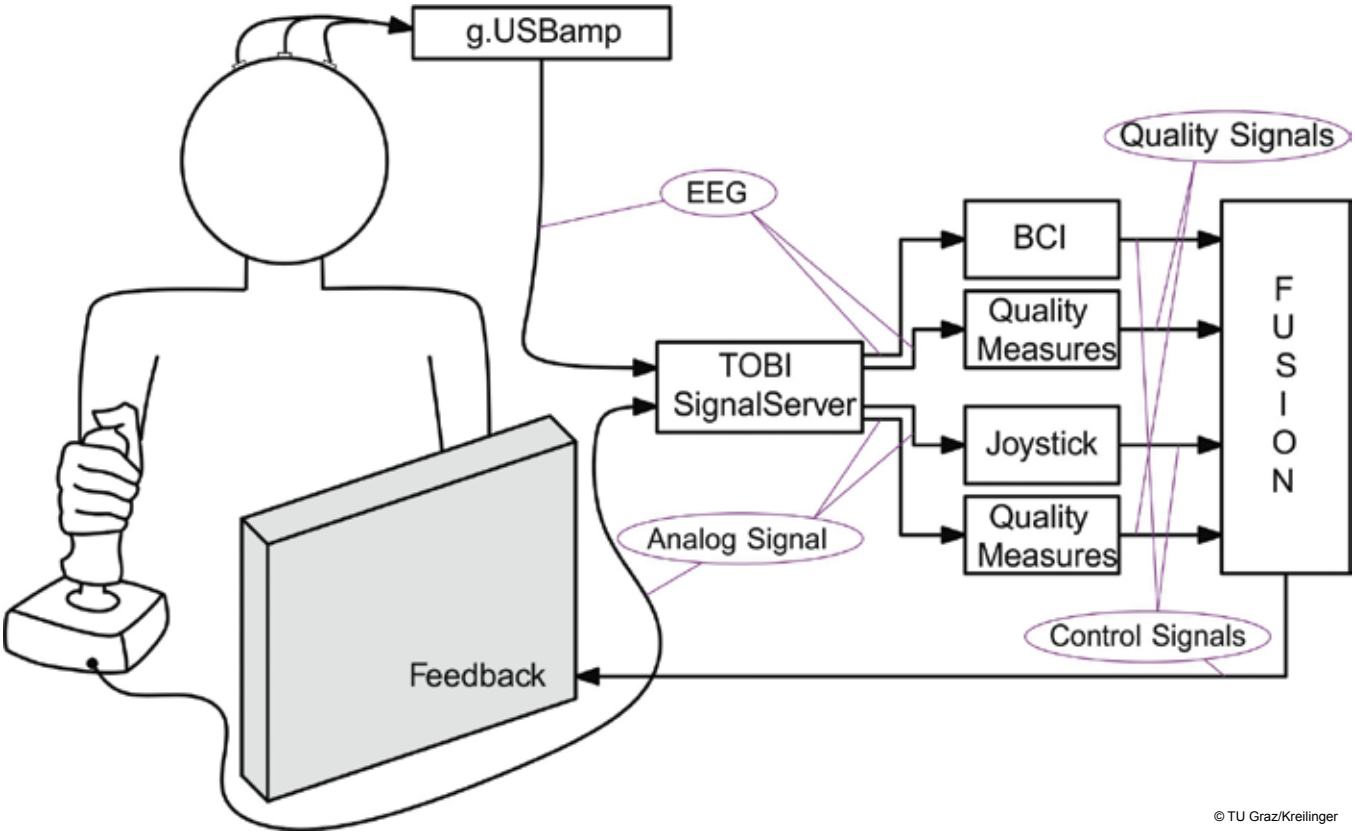


Abb. 2: hBCI kombiniert Joystick und BCI.

Fig. 2: hBCI realized with a joystick and BCI.

Das Prinzip eines solchen hBCI kann man in Abb. 1 sehen. Neben dem EEG-basierten BCI gibt es noch weitere Eingangspfade. Dies können weitere Biosignale und auch andere Steuersignale (z. B. von assistierenden Hilfsmitteln) sein. In der „Fusion“ wird aus allen gleichzeitig vorhandenen Eingangssignalen ein Steuersignal generiert. Dabei werden neben Qualitätskontrollen (z. B. Artefakte) die Signale bewertet und entweder zu einem Steuersignal zusammengefasst oder nur ein sehr sicheres ausgewählt. In der sogenannten „Shared Control“ werden noch Sensorsignale von der jeweiligen Anwendung (Neuroprothese, Software, Assist Robot) zur Bewertung des vom Benutzer/von der Benutzerin kommenden Steuersignals mit einbezogen und so das endgültige Steuersignal erzeugt.

Das hauptsächliche Ziel ist, das hBCI so weit zu bringen, dass eine maximale Anzahl von Szenarien in einer einfachen Art und Weise realisiert werden kann. Um dies zu erreichen, muss das hBCI fähig sein, über einen langen Zeitraum korrekt zu arbeiten, d. h. also, es muss Änderungen erkennen und sich dahingehend anpassen. Um dies zu ermöglichen, müssen viele einzelne Systeme im hBCI miteinander arbeiten können. Beispiele für solche Module sind die EEG- und Biosignalverarbeitung, Postprocessing (z. B. Fehlerpotenziale), Erkennung des mentalen Zustands (z. B. Müdigkeit), Artefakterkennung, Adaption von Klassifikatoren, Qualitätskontrolle der Eingangssignale und u. v. a. Als Beispiel wurde das hBCI als Kombination von

artifact detection), those signals will be weighted and fused to a control signal, or the most reliable one will be chosen. In the so-called “shared control”, sensor signals from the application (neuroprosthesis, software, assistive robot) will also be included and used to generate an accurate final control signal.

One major goal is to bring the BCI technology to a level where it can be used in a maximum number of scenarios in a simple way. To achieve this, the hBCI must be able to operate reliably for long periods, recognizing and adapting to changes as it does so. Achieving this goal requires that many different subsystems in the hBCI are able to work together. Examples include standard BCI processing, post processing (error potentials), mental state recognition (fatigue), artifact detection, adaptation of classifiers, and surveillance of signal quality (including EEG signals and those from additional input devices).

One hBCI fused a commercial joystick and BCI to control a car-game, based on quality measures that constantly monitor and evaluate input signals (see Fig. 2). This observation results in a quality rating. A low quality for the currently active control mode triggers the system to switch to the other mode if its quality rating is better, and therefore promises better performance. To test the system in healthy test users, the joystick signal was deteriorated artificially to simulate weakness, tremors and spasms (impairments likely to appear in patients).

Joystick- und BCI-Kontrolle zur Steuerung eines Autospiels verwendet. Hier werden die Eingangssignale mit Qualitätsmaßen überwacht und evaluiert (Abb. 2). Bei schlechter Qualität des aktuell verwendeten Signals kann zum anderen Kontrollmodus gewechselt werden, insofern dieser eine bessere Qualität vorweisen kann. Um das Modell an gesunden Probanden/Probandinnen zu testen, wurde das Joysticksignal künstlich verschlechtert. Hierzu wurden Muskelschwäche, Tremor und Spasmen simuliert. Beeinträchtigungen, die bei der Anwendung mit Patienten/Patientinnen zu erwarten sind. Durch die Umschaltmöglichkeit waren die Probanden/Probandinnen auch nach völliger Funktionslosigkeit des Joysticks noch in der Lage, das Auto zu kontrollieren. Aufgrund einer Regeneration inaktiver Signale war es auch bei qualitativ schlechtem BCI möglich, wieder in den Joystickmodus zurückzuwechseln.

Eine Folgerung daraus ist in Abb. 3 dargestellt. Ein Proband benutzt zur Steuerung der assistiven Software eine Mundmaus, wobei der Klick mit einem einfachen Hirnsignal realisiert wird. Wird Mundsteuerung zu ungenau, dann schaltet das hBCI in den sogenannten Radar-Maus-Modus, bei dem nur der (BCI)-Klick notwendig ist. Somit kann der gesamte PC gesteuert werden.

Die Entwicklung des hBCI stellt einen weiteren Meilenstein in der BCI-Forschung dar und sie wird dem BCI ermöglichen, als reelles assistierendes Hilfsmittel Einzug in den Patientenalltag zu finden.

Since participants could switch to BCI control, they could control the car even after joystick control was no longer functional. Since joystick control might improve during inactive periods, it was also possible to revert back to joystick control if the BCI no longer provided superior control.

The resulting system is shown in Fig. 3. A person is using a mouth mouse for controlling the assist software, whereas the click function is provided with a BCI. When mouse signals become unreliable, the hBCI switches the mode of the software to radar mouse control, where the mouse can be controlled by clicks only and so the PC can be controlled easily.

Hence, hBCI development is critical in BCI research. hBCIs provide a mechanism to make ADs much more practical, which can allow BCI technology to be used in patients' daily lives.

Abb. 3: hBCI-Benutzer mit Mundmaus und BCI zur Softwarebedienung.

Fig. 3: hBCI user using a mouth mouse and a BCI for software control.

Programmierung ist ein Spiel

Programming is a Game

Roderick Bloem, Krishnendu Chatterjee

Roderick Bloem ist Professor für Informatik am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der Technischen Universität Graz und Sprecher des Nationalen Forschungsnetzwerks für Rigorous Systems Engineering. Er promovierte 2001 an der University of Colorado in Boulder. Seine Forschungsschwerpunkte sind sichere und fehlerfreie Systeme.

Roderick Bloem is a professor of computer science at the Institute for Applied Information Processing and Communications, Graz University of Technology, and is the speaker of the FWF National Research Network on Rigorous Systems Engineering. He received his PhD from the University of Colorado at Boulder in 2001. His research interests are in secure and correct systems.

Computer sind überall: Computer kennen wir meist als Laptops und PCs, doch auf jeden klassischen Computer kommen bereits 50 andere als Bestandteil von Artikeln des täglichen Gebrauchs, von Bankomatkarten bis hin zu Flugzeugen. Computer haben unser Leben zwar einfacher gemacht, doch sind wir stark davon abhängig, dass sie auch fehlerfrei funktionieren. Man denke nur an die Bremse im Auto oder an die kritische Infrastruktur eines Landes: 2003 legte ein Computerfehler die Stromversorgung für 55 Millionen Amerikaner und Amerikanerinnen lahm.

Gleichzeitig tauchen immer mehr Computer in Netzwerken auf. Wenn die Programmierung eines einzigen Computers bereits schwierig ist, um wie viel schwieriger ist die Programmierung eines gesamten Netzwerks. Das menschliche Gehirn ist nun einmal nicht dafür geschaffen, sich über Maschinen Gedanken zu machen, die sequenziell und völlig starr reagieren. Dazu eine Anekdote über ein US-amerikanisches Gesetz, das die Fahrsicherheit von Zügen bei einer Eisenbahnkreuzung gewährleisten soll: „Wenn sich zwei Züge einem Kreuzungspunkt nähern, sollen beide anhalten und so lange nicht weiterfahren, bis der andere die Kreuzung verlassen hat“. Das Gesetz ist eindeutig Unsinn, doch stört dies nicht weiter, solange Menschen daran beteiligt sind – sie werden schon einen gemeinsamen Nenner finden. Diese Flexibilität fehlt jedoch bei Rechnern völlig. Im **Nationalen Forschungsnetzwerk Rigorous Systems Engineering (RiSE)** beschäftigen wir uns mit Methoden, die es auf lange Sicht ermöglichen, fehlerfrei zu programmieren. Im RiSE suchen neun Vollzeitwissenschafter und -wissenschafterinnen und mehr als 20 Nachwuchswissenschafter und -wissenschafterinnen nach Wegen, die Qualität von Softwareprogrammen zu verbessern. In diesem Artikel werden wir uns mit

Computers are most visible as laptops and PCs, but for each “classical” computer, there are 50 computers embedded in everyday items from ATM cards to airplanes. Computers have made are our lives much easier, but we also depend greatly on their functioning correctly. Computer programs that are responsible for the brakes in a car or the critical infrastructure of a country must be programmed correctly. This is not always the case: for instance, a computer error contributed to the 2003 power blackout in the North America, which affected 55 million people.

At the same time, computers increasingly appear in networks. Where programming one computer is hard, programming a network of computers is extremely hard. The human mind is simply not equipped to reason about machines that act concurrently without any flexibility. An apocryphal story tells of a US state law to control the safe behaviors of trains at an intersection: “When two trains approach an intersection, both shall come to a full stop, and neither shall move until the other is gone.” The law is clearly nonsensical, but that is not a problem when humans are involved – they will work something out. Computers, however, lack that flexibility and when confronted with the computer equivalent of such a rule, will grind to an interminable halt.
In the **NFN’s Rigorous Systems Engineering (RiSE)**, we study methods to systematically design error-free programs. In RiSE, nine primary investigators and over 20 junior researchers study ways to improve the quality of software. In this article, we will look at the theory of correct programming and describe one approach, synthesis, which builds on game theory.

Abb. 1: Die Überprüfung der Fehlerfreiheit der Software kann mittels der Spieltheorie erfolgen.

Fig. 1: Checking correctness of software can be done using game theory.

der Theorie des richtigen Programmierens beschäftigen und einen spieltheoretischen Ansatz beschreiben, die Synthese.

Programmieren heißt, ein Spiel korrekt aufzulösen

Grundsätzlich geht es beim Programmieren darum, Spiele zu *lösen:* eine Spielanleitung zu schreiben, sodass man immer gewinnt. Manche Spiele sind leicht zu lösen. Die meisten Leute spielen perfekt „Tic Tac Toe“ („Drei gewinnt“) – sie verlieren nie, egal, gegen welchen Gegner. Auch das Spiel „Vier gewinnt“ wurde bereits gelöst. Es gibt eine Taktik, mit welcher die Person, die beginnt, immer gewinnt. (Und demgemäß keine, mit welcher der zweite Spieler immer gewinnt.) Spiele wie Schach sind jedoch außer Reichweite. Zwar sind Schachprogramme mittlerweile extrem ausgereift und können fast jeden schlagen, Gewinngarantie gibt es jedoch keine, und genau darum geht es uns hier.

Der Zusammenhang zwischen dem Lösen von Spielen und dem Schreiben von Programmen ist eng. Während der Ausführung erhält das Programm Inputs, z. B. von einer Benutzerin, die Tasten drückt. Es produziert Outputs: Pixel auf einem Schirm, Geräusche oder Netzwerktraffic. Entscheidend ist dabei, dass das Programm immer fehlerfrei abläuft und nie ein falsches Ergebnis generiert. Daher sehen wir Umwelt und Programm als zwei gegnerische Spieler: Das Programm versucht, alles richtig zu machen, während die Um-

Programming is solving a game

At the foundations, programming is like *solving* a game: writing a recipe that tells you how to play a game so that you will never lose. Some games can be solved easily. Most people are perfect players at tic-tac-toe – they will never lose, no matter how good the opponent. The game “connect-four” has also been solved. There is a recipe for the beginning player to always win. (Consequently, there is no recipe that allows the second player to always win.) Games like chess, however, are beyond reach. Computer programs have become extremely strong at chess, and can beat almost any player, but there is no guarantee that they win, and that is what we are after.

The connection between solving games and writing computer programs is close. During its execution, a computer program receives inputs from the environment, for instance from a user who presses buttons. It produces outputs: pixels on a screen, sounds, or network traffic. It is crucial that the program is correct under any circumstance and never produces a wrong output. Thus, we consider the environment and the program as opposing players: the program tries to do everything right, whereas the environment tries to provide inputs that are impossible to react to. Typically, inputs and outputs alternate like moves in chess. The rules of the game are given by a specification that states which outputs are allowed when and the system wins if it fulfills the specifications.

Krishnendu Chatterjee ist Assistent Professor am Institute of Science and Technology (IST) Austria. Er promovierte 2008 an der University of California in Berkeley. 2008 erhielt er auch den Ackerman Award für die weltweit beste Dissertation in Computerlogik. Sein Forschungsschwerpunkt sind die theoretischen Grundlagen der formellen Verifikation und Spieltheorie.

Krishnendu Chatterjee is an assistant professor at the Institute of Science and Technology (IST) Austria. He received his PhD from the University of California, Berkeley in 2008. He is the receiver of the 2008 Ackerman Award for the best thesis worldwide in computer science logic. His main research interest is in the theoretical foundations of formal verification and game theory.

Abb. 2: Das Team von RiSE (v.l.n.r.) Thomas A. Henzinger, Christoph Kirsch, Ulrich Schmid, Helmut Veith, Armin Biere, Roderick Bloem, Uwe Egly, Laura Kovács, Krishnendu Chatterjee.

Fig. 2: The team of RiSE (from left to right: Thomas A. Henzinger, Christoph Kirsch, Ulrich Schmid, Helmut Veith, Armin Biere, Roderick Bloem, Uwe Egly, Laura Kovács, Krishnendu Chatterjee.

welt versucht, Inputs zu liefern, auf die es nicht reagieren kann. Typischerweise wechseln sich Inputs und Outputs ab, wie Spielzüge im Schach. Die Spielregeln definieren eine Vorgabe darüber, welche Outputs wann erlaubt sind, und das System gewinnt, wenn es alle Vorgaben erfüllt.
Nehmen wir zum Beispiel eine Druckersteuerung. Die Vorgabe könnte lauten, dass

1. Druckaufträge eine Sekunde in Anspruch nehmen dürfen,
2. jeder Auftrag in zwei Sekunden abzuarbeiten ist und
3. keine zwei Druckaufträge gleichzeitig abgearbeitet werden dürfen (um Kollisionen zu vermeiden).

Wenn das System drei Nutzerinnen hat, kann diese Vorgabe unmöglich erfüllt werden – wenn jede Nutzerin zur gleichen Zeit einen Druckauftrag startet, *muss* das System eine der drei Anforderungen verletzen. Ändern wir Vorgabe zwei jedoch dahingehend, dass die Aufträge in bis zu drei Sekunden abzuwickeln sind, so kann die Vorgabe erfüllt werden. Die Druckersteuerung stellt sicher, dass alle Regeln eingehalten werden, unabhängig davon, wie sich die Umwelt verhält.

Fehlerfreiheit gewährleisten

Es gibt mehrere Möglichkeiten, um zu gewährleisten, dass Softwareprogramme fehlerfrei ablaufen. Der übliche Weg ist, sie zu testen. Beim **Testen** probieren wir verschiedene Inputs aus und überprüfen, ob auch die Outputs stimmen. Aus der Analogie mit dem Spiel wird jedoch deutlich, dass diese Vorgangsweise nicht ideal ist. Die Tatsache, dass Sie 1, 2 oder eine Million Spiele verlieren, bedeutet nicht, dass Ihr Gegner unfehlbar ist und gegen jedermann gewinnen würde.
Eine systematischere Möglichkeit, fehlerfreies Funktionieren zu gewährleisten, ist die **Verifikation.** Dabei wird ein Beweis dafür aufgebaut, dass ein bestimmtes Programm fehlerfrei abläuft,

An example would be an arbiter for a printer. The specification may say that

1. Print jobs take one second,
2. Each job must be handled within two seconds, and
3. Two print jobs may not be served at the same time (lest garbage ensues).

If there are three users of the system, this specification cannot be fulfilled by any system – if each user issues a print job at the same time, the system *must* violate one of the three requirements. If we change requirement 2 to state that jobs can take up to three seconds to be completed, the specification can be satisfied: there is an arbiter that fulfills all the rules regardless of the behavior of the environment.

Ensuring correctness

There are multiple ways to make sure that software works correctly. The usual way is **testing**. When testing a program, we try many different inputs and check that the outputs are correct. It is clear from the game analogy that this approach is not ideal. The fact that you lose 1, or 2, or a million games does not mean that your opponent is infallible and would win against anyone. The main reason to perform tests is that a first indication of a program's correctness can be obtained very quickly.
Verification is a systematic way to ensure correctness. We construct a proof that a given program is correct regardless of the inputs. This approach has great appeal because we can gain complete confidence in the program. It is like making sure that a player is perfect. The drawback is also clear: it is not easy to see that a strategy is perfect, and constructing a proof of correctness may be hard. Still, the community has made tremendous progress in this field over the last 2 decades. So-called model checkers can automatically construct proofs of correctness for programs

unabhängig von den Inputs. Wir können damit große Sicherheit in der Richtigkeit des Programms erreichen, so, als würden wir uns versichern, dass ein Spieler oder eine Spielerin perfekt ist. Der Nachteil ist, dass es nicht leicht ist zu beweisen, dass eine Strategie bzw. ein Programm perfekt ist. Die Softwarecommunity hat im Laufe der letzten 2 Jahrzehnte aber beträchtliche Erfolge erzielt. Sogenannte Model Checker sind heute in der Lage, automatisch den Nachweis der Fehlerfreiheit für so kleine, aber wichtige Programme wie Gerätetreiber zu liefern.

Ein Nachteil der Verifikation besteht darin, dass Benützer/Benützerinnen sowohl ein fehlerfreies Programm als auch eine perfekte Vorgabe erstellen müssen. Idealerweise sollte es genügen, eine gute Vorgabe zu schreiben, woraus ein fehlerfreies Programm automatisch erstellt wird. Dieser Ansatz, **Synthese** genannt, ist die Königsklasse in Sachen Fehlerfreiheit. Doch nun zurück zur Analogie mit dem Spiel: In der Synthese wird versucht, automatisch einen perfekten Spieler zu konstruieren, der jeden Gegner bezwingt. Genau darum geht es in der Spieltheorie.

Bis vor fünf oder zehn Jahren galt die Synthese als von rein theoretischem Interesse; man war skeptisch, Real-Life-Systeme aufgrund von Vorgaben automatisch generieren zu können. Die letzten fünf Jahre haben uns diesem Ziel jedoch erheblich näher gebracht. Innovative Konzepte der Spieltheorie ermöglichen es uns, die Fähigkeiten von Synthesetools auf kleine, aber realistische industrielle Systeme auszudehnen. Das ist zweifellos ein großer Erfolg, der umso spannender ist, als er viele neue und unerwartete theoretische Fragen aufwirft – über die richtige Sprache der Vorgabe, das Erfordernis der Robustheit usw. Diese Fragen an der Schnittstelle zwischen Theorie und Praxis sind Kernthemen des RiSE-Netzwerks und, wie wir meinen, ein wichtiger Meilenstein auf dem Weg zur Programmierung fehlerfreier Systeme.

like device drivers (which are small but may create large problems).

Another drawback of verification is that the user must construct both a working program and a perfect specification. Ideally, it should suffice to write a good specification; a correct program should then be constructed automatically. This approach, called **synthesis**, is the major league of correctness. Returning to the game analogy, synthesis attempts to construct a perfect player automatically, a player that wins against any opponent. This problem is the topic of game theory, a discipline that originates from economics. Up to 5 or 10 years ago, synthesis was considered to be only of theoretical interest; it was considered completely unrealistic to construct real-life systems automatically from specifications. Over the last five years, however, we have made tremendous progress towards this goal. Using novel game-theoretic concepts, we have been able to extend the capability of synthesis tools to small, but realistic industrial systems. This is a great success, and it is even more exciting as it raises many new and unexpected theoretical questions concerning the right specification languages, the need for robustness, etc. These new questions on the intersection between theory and practice will be one of the topics of the RiSE network, and we expect them to be an important cornerstone in future approaches to programming correct systems.

RiSE

Rigorous Systems Engineering ist ein vom FWF finanziertes nationales Forschungsnetzwerk. Das Projekt bündelt die Kompetenzen von Weltklasseforschern und -forscherinnen für Verifikation in Österreich: Armin Biere (JKU Linz), Roderick Bloem (TU Graz, Sprecher), Krishnendu Chatterjee (IST Austria), Uwe Egly (TU Wien), Tom Henzinger (IST Austria), Christoph Kirsch (PLU Salzburg), Laura Kovács (TU Wien), Ulrich Schmid (TU Wien) und Helmut Veith (TU Wien).

RiSE

Rigorous Systems Engineering is an FWF-funded National Research Network. The project bundles the strengths of world-class researchers in verification in Austria: Armin Biere (JKU Linz), Roderick Bloem (Graz University of Technology, speaker), Krishnendu Chatterjee (IST Austria), Uwe Egly (TU Wien), Tom Henzinger (IST Austria), Christoph Kirsch (PLU Salzburg), Laura Kovács (TU Wien), Ulrich Schmid (TU Wien), and Helmut Veith (TU Wien).

E-Learning an der TU Graz – Von der Forschung in die Praxis als Gesamtstrategie

E-Learning at Graz University of Technology – From Research to Practice as Strategy

Martin Ebner

Martin Ebner ist Leiter der Abteilung Vernetztes Lernen am Zentralen Informatikdienst der TU Graz und Dozent am Institut für Informationssysteme und Computer Medien.

▶ http://elearning.tugraz.at

Martin Ebner is head of the department of Social Learning at Computer and Information Services and associate professor at the Institute of Information Systems and Computer Media.

▶ http://elearning.tugraz.at

Die Abteilung Vernetztes Lernen des Zentralen Informatikdienstes wurde mit der Aufgabe gegründet, E-Learning an der TU Graz zu etablieren. Hierzu gibt es eine strategische Ausrichtung, die durch mehrere Protagonisten vertreten und die in diesem Artikel kurz beschrieben wird. Es zeigt sich, dass in einem Forschungsgebiet mit hohem Feldforschungsanteil die Zusammenarbeit mit Instituten Mehrwerte bietet.

Die Vision der TU Graz

Die Abteilung Vernetztes Lernen des Zentralen Informatikdienstes (ZID) wurde 2006 als Arbeitsgruppe gestartet, um digitale Technologien in die Hochschullehre zentral zu integrieren. Die Vision ist, „die Präsenzlehre mit Medien zu bereichern, um damit die Kommunikation zu verbessern und darüber hinaus durch eine zentrale Steuerung auch für Nachhaltigkeit zu sorgen". Hingewiesen sei dabei auf die Stichworte bereichern, Kommunikation, zentral und Nachhaltigkeit. Das bedeutet, dass die vorherrschende Präsenzlehre nicht von digitalen Technologien verdrängt, sondern optimiert und bestmöglich ergänzt wird. Weiters wird versucht, neuartige Kommunikationskanäle anzubieten, Diskussion in der Lehre als ein wesentliches Instrument aufzugreifen und zu fördern. Damit Wartung, Know-how und auch der Datenbestand langfristig gesichert sind, muss die Steuerung zentral erfolgen.

Auf Basis dieser Ausrichtung und der gleichzeitigen Forderung nach einer großen Forschungsnähe begann die vormalige Arbeitsgruppe mit ihrer Arbeit. Durch enge Kooperation zwischen dem ZID und dem Institut für Informationssysteme und Computer Medien (IICM – Vorstand vormals Hermann Maurer, jetzt Frank Kappe), welches schon damals seit vielen Jahren erfolgreich forschte, wurden Ergebnisse unmittelbar in die Praxis übergeführt. In diesem Artikel wird nun ein Überblick über die Gesamtaktivitäten gegeben.

The Social Learning at Computer and Information Services department was founded to establish e-learning at Graz University of Technology. The strategy is based on a number of protagonists and will be described in this article. It can be shown that close co-operation with a research institute is of high benefit in a research topic with a high level of field research.

The Vision of Graz University of Technology

In 2006 the Social Learning at Computer and Information Services department started as a work group to integrate and centralise digital technologies in higher education. The vision is to enhance face-to-face teaching with technologies to improve communication and to foster sustainability through a centralised approach. Crucial terms are enhancement, communication, centralisation and sustainability.

Traditional face-to-face teaching will not be replaced by digital technologies but will be optimised and enhanced. Additionally, new communication channels are offered to allow and foster discussion as an important instrument. Finally, maintenance, know-how and data storage must be centralised.

This approach and the demand for proximity to research provided the point of departure of the former work group. Through close co-operation between the Computer and Information Services and the Institute of Information Systems and Computer Media (IICM – former head Hermann Maurer, present head Frank Kappe), which had been conducting e-learning research for many years, results were put into practice. In this article, we will give a short overview about the salient activities.

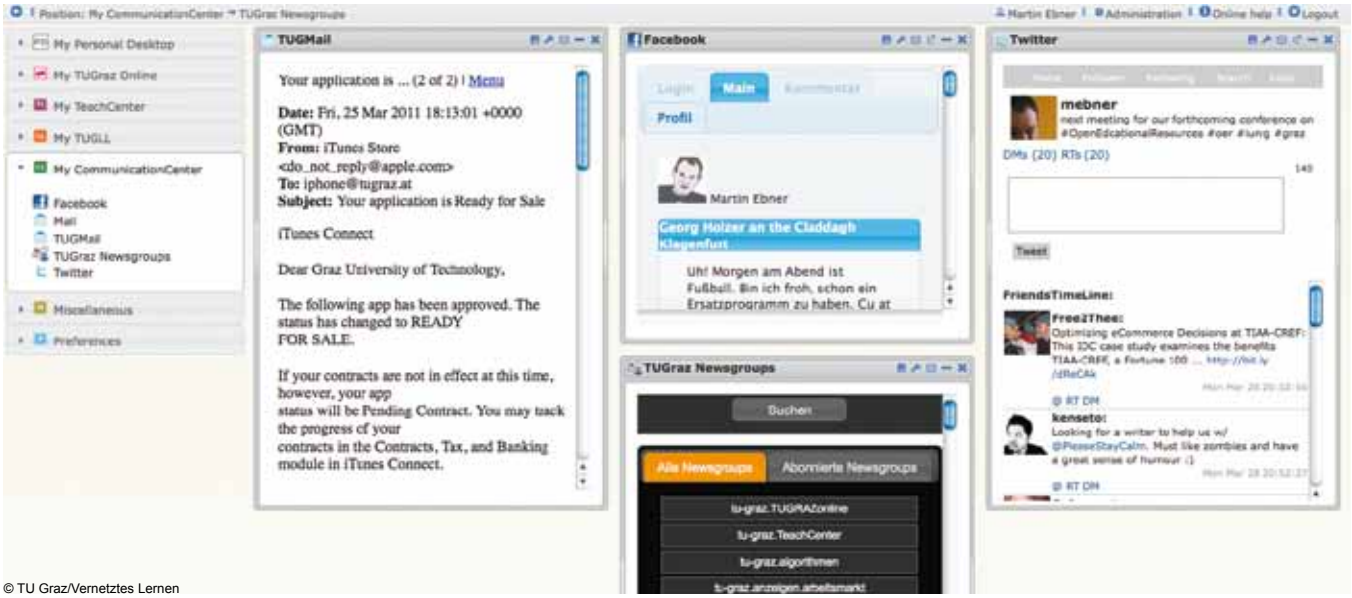


Abb. 1: Personal Learning Environment der TU Graz.

Fig. 1: Personal Learning Environment.

TU Graz TeachCenter – der Lehrende im Mittelpunkt

Standard ist, dass eine österreichische Hochschule ein Lernmanagementsystem (LMS) anbietet. LMS helfen auf digitalem Wege, Lehrveranstaltungsinhalte und Lehrszenarien strukturiert anzubieten. Darüber hinaus können Lernende über ein LMS üblicherweise ihre Abgaben tätigen, über auftretende Fragen diskutieren, sich digital zu Gruppen finden, Überprüfungen durchführen und vieles mehr. Das LMS erweitert den Präsenzunterricht, indem es Lehrende für die Lernenden in didaktisch sinnvoller Weise einsetzen. Die TU Graz setzt hierbei das Open-Source-System WBT-Master, genannt „TU Graz TeachCenter", ein, das am IICM entwickelt worden ist und laufend angepasst wird.

▶ http://tugtc.tugraz.at

Personal Learning Environment (PLE) – der Lernende als zentrale Figur

Beim LMS bereiten Lehrende ihre Inhalte unter Berücksichtigung didaktischer Gesichtspunkte für Lernende auf. Die individuellen Bedürfnisse der Lernenden bleiben davon aber unberührt.

Die PLE setzt hier an und bietet den Lernenden die Möglichkeit, Vorlieben und Lerngewohnheiten zu berücksichtigen. Mithilfe sogenannter Widgets können verschiedenste Webdienste und Services nach Belieben über die PLE kombiniert werden. Je nach Verfügbarkeit solcher Widgets können so universitätsweite Angebote (zum Beispiel TUGraz.online) sowie auch universitätsexterne Webangebote (zum Beispiel Twitter) nach eigenen Vorstellungen zusammengestellt werden (siehe Abb. 1). Eine PLE zielt also auf eine stark selbstgesteuerte Lerntätigkeit ab, die sich kurzfris-

TU Graz TeachCenter – the teacher in focus

A Learning Management System (LMS) is already standard at Austrian universities. With the help of an LMS, teaching content and scenarios can be offered in a digital way. Furthermore, students are able to upload homework, discuss open questions, find groups and fill out self-assessments, etc. An LMS enhances the face-to-face teaching by assisting teachers offering well-prepared courses. At Graz University of Technology, the open-source system WBT-Master, called "TU Graz TeachCenter" and developed at IICM, is being continuously used and adapted.

▶ http://tugtc.tugraz.at

Personal Learning Environment (PLE) – the learner as central player

With the help of an LMS, teachers are offering content in an appropriate didactic way. The individual needs of learners are marginally considered. A Personal Learning Environment gives learners an opportunity to integrate their personal learning requirements. So-called widgets allow the combination of different web services and applications. If such widgets are available, both university-wide services (for example TUGraz.online) and external services (for example Twitter) can be brought together (see Fig. 1). A PLE aims at self-directed learning activities, short term in information provision and long term in information processing.

▶ http://ple.tugraz.at

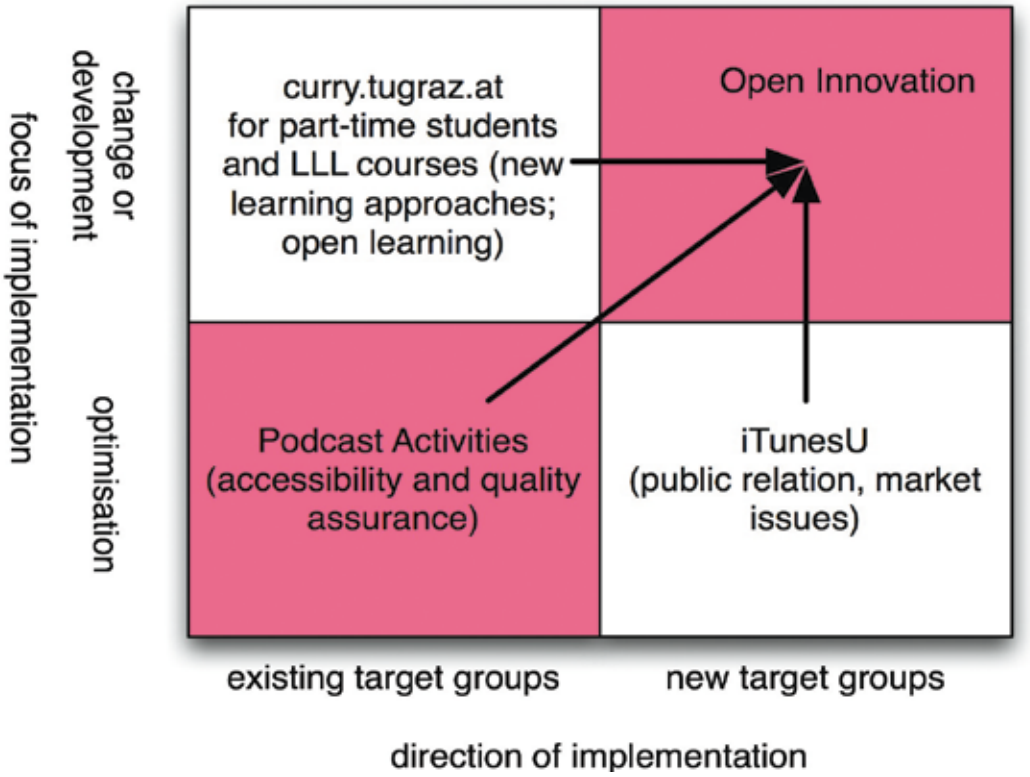


Abb. 2: Open-Content-Strategie der TU Graz.

Fig. 2: Open Content Strategy.

tig in einer Informationsaufbereitung und langfristig in einer Informationsverarbeitung abbildet.

- http://ple.tugraz.at

Open Content – die Öffentlichkeit im Blickpunkt

Ein wesentlicher Bestandteil der Strategie ist, dass Bildungsmaterialien grundsätzlich frei zugänglich sind. Die weltweite von der UNESCO ausgehende Initiative zu Open Educational Resources (OER) ist deswegen relevant, weil damit Potenziale bei der Vereinfachung von Prozessen, Einsatz von neuen offenen Lern- und Lehrformen, Innovationsentwicklung, Möglichkeiten der PR sowie auch neuartige Formen der organisationsübergreifenden Vernetzung und Kollaboration geschaffen werden können. Dies wurde zum Anlass genommen, als erste österreichische Universität OER strategisch zu verankern (siehe Abb. 2) und sämtliche freie Bildungsangebote gesammelt auf einer Webseite darzustellen:

- http://opencontent.tugraz.at

Besonders erwähnt gehören hier die aktive Mitarbeit bei iTunes U

- http://itunes.tugraz.at

sowie das Angebot von Live-Streams und Vorlesungsaufzeichnungen auf

- http://curry.tugraz.at

Des Weiteren ist die Abteilung maßgeblich an der Open-Access-Veröffentlichung des Lehrbuchs „Lehren und Lernen mit Technologien“

- http://l3t.eu

Open Content – the perspective of society

A crucial part of the strategy is open educational resources. The worldwide initiative, coming from UNESCO, is important to establish potentials of simplifications, usage of new and open learning formats, innovation development, opportunities for public relations as well as inter-organisational cooperations and collaborations. Due to this, Graz University of Technology was the first Austrian university with a strategic integration (see Fig. 2) and the first to collect all open educational resources on one webpage:

- http://opencontent.tugraz.at

Especially the iTunesU activities

- http://itunes.tugraz.at

and live-streams as well as lecture recordings

- http://curry.tugraz.at

have to be mentioned. Furthermore, the department is significantly involved in an innovative, open-access, e-learning textbook project

- http://l3t.eu

and hosts two important open-access journals in the German speaking area in the field of educational research and teaching:

- http://bildungsforschung.org
- http://zfhe.at

Research trends

Research in e-learning is driven from both an interdisciplinary and technological level. Currently, there is a trend towards mobile devices and mobile Internet, which will influence learning and

beteiligt und hostet zwei große Vertreter der deutschsprachigen Open-Access-Fachzeitschriften: die Bildungsforschung

- http://bildungsforschung.org

und die Zeitschrift für Hochschulentwicklung.

- http://zfhe.at

Forschungstrends

Die Forschung im Bereich E-Learning ist zum einen gekennzeichnet von ihrer Interdisziplinarität und zum anderen vom technischen Fortschritt. So ist derzeit ein Trend hin zu mobilen Endgeräten und mobilem Internet erkennbar, der mittelfristig auch das Lehren und Lernen beeinflussen wird.

Die Abteilung führt in diesem Kontext zusammen mit dem IICM Entwicklungen sowie auch Feldversuche durch. Beispielhaft können hier die Programmierung von iPhone-Apps für die Lehre (siehe Abb. 3) und auch der Einsatz des großen sozialen Netzwerks Twitter für Echtzeitrückmeldungen im Hörsaal

- http://twitterwall.tugraz.at

genannt werden. Weiters gibt es massive Bemühungen, die Erstellung von Lehrunterlagen als E-Books zu forcieren. Digitale Skripten werden unter Verwendung einer selbst entwickelten Autoren-Software

- http://ebook.tugraz.at

erzeugt und für gängige E-Reader lesbar gemacht.

Zusammenfassung

Das Ziel der TU Graz ist es, durch E-Learning-Elemente die Präsenzlehre nicht zu ersetzen, jedoch bestmöglich zu unterstützen. Dabei wird auch die Rolle der Lehrenden keineswegs zurückgedrängt; vielmehr erfordert es eine sorgfältige Planung, wann und wie moderne Medien Mehrwerte im Unterricht bieten können. Um die Lehre dadurch langfristig zu bereichern und auf diesem doch sehr hohen Niveau halten zu können, sind einerseits Qualitätssicherung und andererseits die Anpassung an neue Forschungsergebnisse notwendig. Durch die gute Kooperation mit dem Institut IICM konnte dies bisher gewährleistet werden.

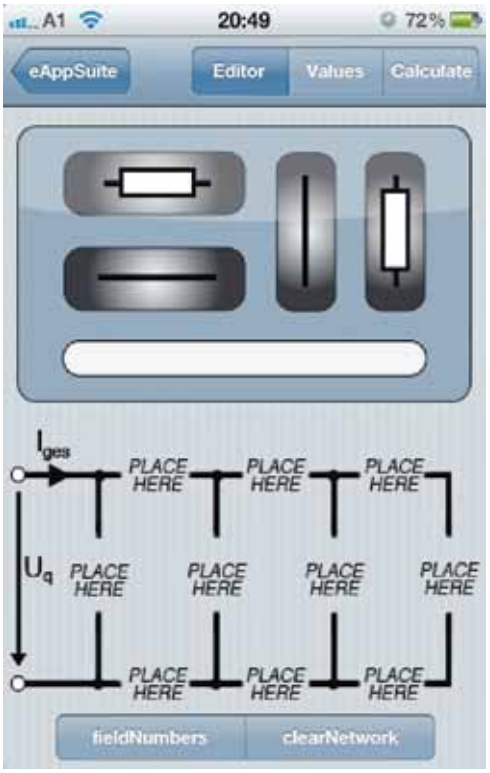


Abb. 3: iPhone-Applikation – eAppSuite.

Fig. 3: iPhone Application – eAppSuite.

teaching significantly in the medium term. Together with the IICM, the department develops applications and carries out field research. Examples are the iPhone development for teaching (see Fig. 3) and the use of the big social network Twitter for in-time comments and feedback in lecture halls

- http://twitterwall.tugraz.at

Furthermore, there is a strong research trend towards creation of e-books as lecture material. Digital lecture notes will be generated with a self-developed authoring software

- http://ebook.tugraz.at

and afterwards readable with the usual e-reader devices.

Summary

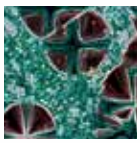
Graz University of Technology is aiming to enhance face-to-face teaching in a meaningful way and not to replace it. The role of teachers is more important than ever and needed for careful planning as well as if and how to use technologies in teaching. To enrich education sustainably and to keep quality at a high level, quality assurance and the integration of new research results is of supreme importance. This is one result of the ongoing fruitful co-operation with the IICM.

Fünf zukunftsträchtige Bereiche in Forschung und Lehre bilden den unverwechselbaren Fingerabdruck der TU Graz auf dem Weg zur Exzellenz. Diese Fields of Expertise sind Kompetenzbereiche, die zu einzigartigen Markenzeichen der TU Graz im 21. Jahrhundert werden sollen. Gestärkt werden die Fields of Expertise durch thematisch neue Professuren und Investitionen sowie intensive Zusammenarbeit mit Industrie und Wirtschaft in Form von zahlreichen gemeinsamen Beteiligungen an wissenschaftlichen Kompetenzzentren und Forschungsnetzwerken. Kooperationen mit wissenschaftlichen Partnereinrichtungen wirken als weiterer Motor zum Erfolg.

Five areas with a promising future in research and teaching go to form the unmistakeable fingerprint of Graz University of Technology on its path to excellence. These fields of expertise will become distinctive hallmarks of Graz University of Technology in the 21st century. They will be strengthened by thematically new professorships and investments as well as intensive co-operation with industry and business in the form of numerous shared participations in scientific competence centres and research networks. Cooperations with scientific partner institutes represent a further dynamo to success.

Information, Computing, and Communication Technologies

Human- & Biotechnology



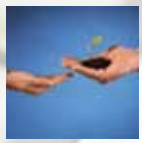
Advanced Materials Science

FOE

Fields of Expertise

Mobility Research and Production Sciences

Sustainability in Design, Construction and Energy Systems



Impressum: Eigentümer: TU Graz. Herausgeber: Büro des Rektorates, Leitung Ursula Tomantschger-Stessl, im Namen des Vizerektors für Forschung und Technologie. Redaktion: Ines Hopfer, TU-research@tugraz.at, Redaktionsadresse: TU Graz, Büro des Rektorates, Rechbauerstraße 12/I, 8010 Graz. Gestaltung/Layout: Christina Frauneder, Satz: B&R Satzstudio, A.R. Reinprecht. Druck: Medienfabrik Graz. Auflage: 4500 Stück. Wir danken den Autorinnen und Autoren für die Bereitstellung der Texte und Fotos. Geringfügige Änderungen sind der Redaktion vorbehalten. Titelbild: istockphoto.com. TU Graz *research* erscheint zweimal jährlich.

ISSN 2074-9643