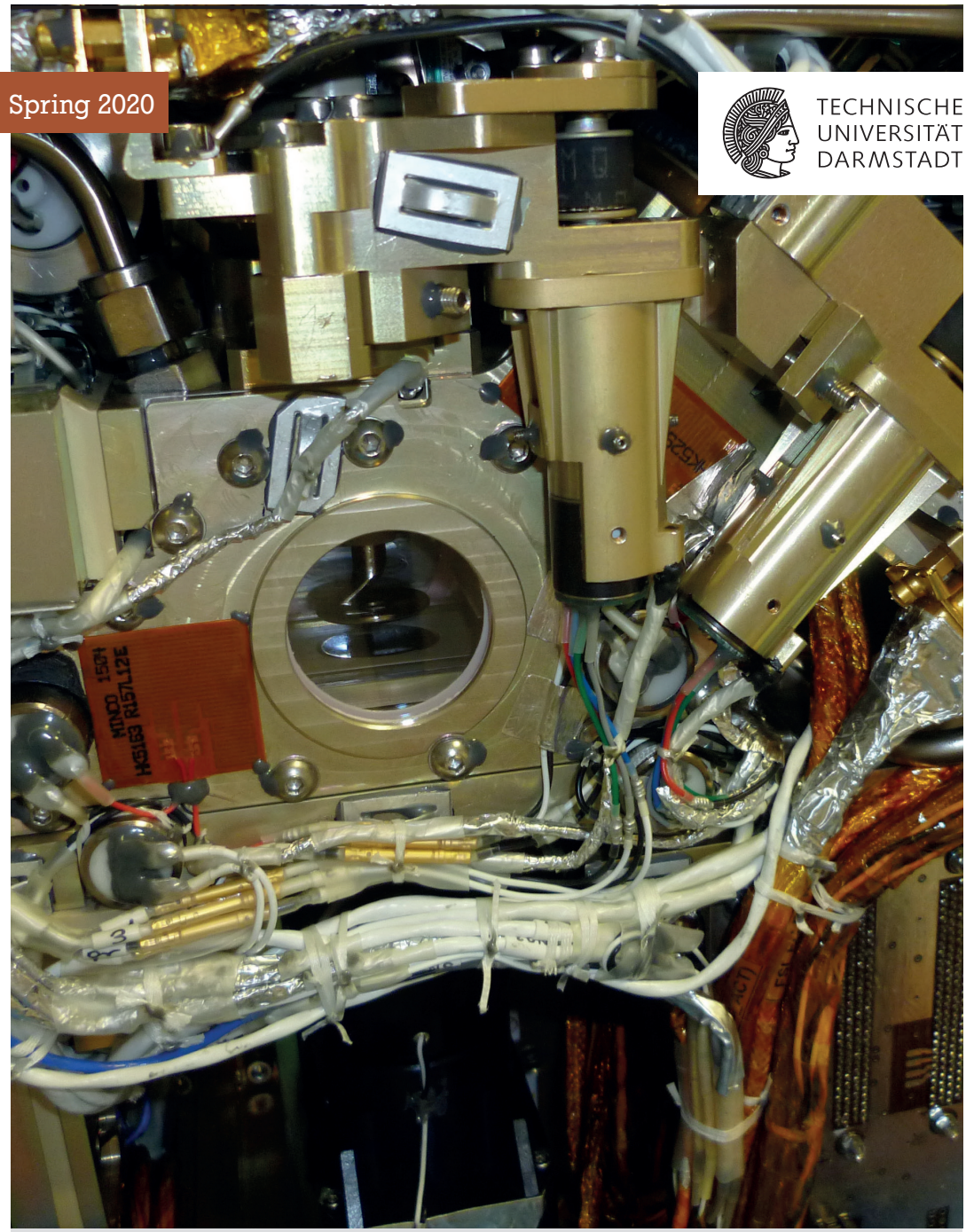
hoch3 FORSCHEN

SCIENCE QUARTERLY

Spring 2020

TECHNISCHE UNIVERSITÄT DARMSTADT



Imprint

Publisher
President of TU Darmstadt,
Karolinenplatz 5,
64289 Darmstadt,
Germany

Editor
Corporate Communication
Jörg Feuck (Editor-in-chief)
Ulrike Albrecht (Graphic Design)
Patrick Bal (Images)

Title
Close-up of the Experimental Cell in the Experimental Container; Photography: Airbus Defence and Space

Printing
Druckerei Petzold GmbH, Darmstadt
printed on 100 g/m² PlanoScript, FSC-zertificated

Circulation 5.000

Next issue 15th June 2020

Service for readers
presse@pvw.tu-darmstadt.de

Newsletter subscription
www.tu-darmstadt.de/newsletter

ISSN
2196-1506

Would you like to receive the next issue of hoch³FORSCHEN? Please send an E-Mail to presse@tu-darmstadt.de

A better poker face for computers

Spectacular security loopholes discovered in modern processors are setting new challenges for scientists: Computer Science Professor Heiko Mantel and his team are studying the danger of difficult to detect attacks via so-called side channels and possible countermeasures.

Photography: Katrin Binner

Alexandra Weber, Dr. Damien Marion and Professor Heiko Mantel (from left to right) are performing a side-channel analysis.

By Ann-Kathrin Braun

"A bad poker face can also be viewed as a side channel", says Professor Heiko Mantel to explain his research on "side channels". In a game of cards, your facial expressions and your body behaviour might reveal to other players a lot about the quality of your cards. Similarly, side-channel attacks in IT-systems leak secret information via channels that were not meant to be used for such communication.

The security of confidential data does not only depend on security mechanisms such as cryptography or access controls. It also depends on restricting the flow of information, meaning where and how information is propagated when running a program. Information-flow control does not exclude access to confidential information, but rather limits how it can be used. Heiko Mantel has been investigating the theme of information-flow security since being a doctoral candidate and on his path to becoming a professor in Computer Science. This theme was the main focus of the Priority Programme "Reliably Secure Software Systems" that he headed, and that was funded by the German Research Foundation (DFG). His work in the CROSSING Collaborative Research Centre at TU Darmstadt builds on this prior work.

"The question is not only whether a system is secure or not, but rather how secure is it?"

The complexity of IT systems has increased considerably over time due to rapid advances in technology. "A major achievement of Computer Science is the ability to think about systems using abstractions. Differentiating between layers of abstraction makes the conceptual complexity of such systems tractable", says Mantel. Thinking in terms of such layers is essential for most applications – after all, software developers, for example, cannot be expected to take all details of the hardware and operating system into account when they are programming. However, thinking only within abstraction layers creates "an open door for side channels". The betrayal of secrets does not have to take place within a single system layer: "Side channels do not obey the rules of abstraction", emphasises the computer scientist.

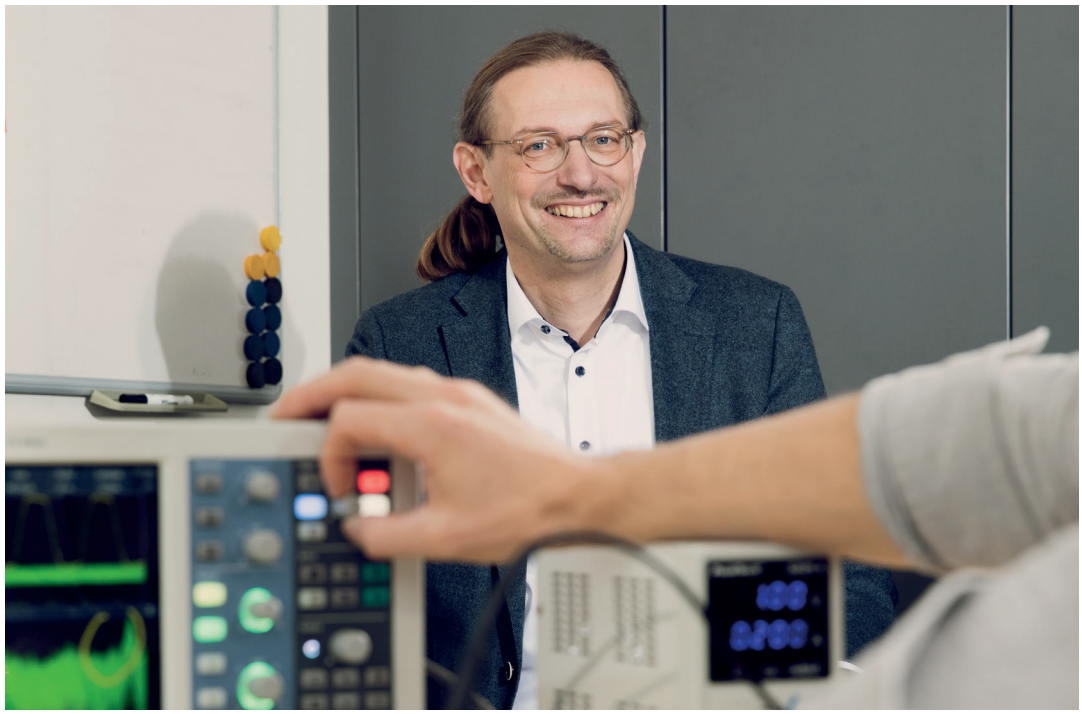
In a poker game, you can exploit the side channel "facial expression", that is, the bad poker face of other players. In Computer Science, side channels can be established based on other more technical characteristics, such as the emanation of heat, processing time, electromagnetic waves, sounds, or power consumption. The research in Mantel's group focuses on side-channel attacks that do not require any physical access and, hence, are particularly dangerous. To identify them, the scientists in the CROSSING Collaborative Research Centre pursue multiple approaches.

Firstly, they employ formal methods: This allows one to understand and analyse a program's behaviour based on precise, mathematical models. Describing models in natural language would not be sufficiently precise for obtaining reliable, unambiguous analysis results. After all, a security guarantee should not be interpretable in different ways.

Following this approach, the objective is to determine upper bounds on how much secret information might be betrayed to others. The doctoral candidate Alexandra Weber is working on this subject at Mantel's chair. "I can determine how much of a

Information

Computer Science
Prof. Dr.-Ing. Heiko Mantel
Phone: +49(0)6151/16–25252
Email: mantel@cs.tu-darmstadt.de
http://www.mais.informatik.tu-darmstadt.de



Photography: Katrin Binner

The power consumption of hardware components can be measured using an oscilloscope, and this information can be used for side-channel attacks.

secret might be leaked in a worst case scenario.", says the young scientist. "I find it very motivating that my research allows me to provide such precise and reliable security guarantees." For instance, if a cryptographic key consists of 256 bits, the formal approach can be used to calculate how many bits might be leaked to an attacker via a side channel at most. "In the process, the mathematical model defines where information is permitted to flow, what the secrets are, and what the attacker is able to "see"", according to Weber. The aim of the research in CROSSING is to create tools for analysing software with respect to side channels automatically.

It was already possible to semi-automatically identify such loopholes in a very successful interdisciplinary cooperation between the research group headed by Professor Mantel and the team "q-TESLA". q-TESLA is a post-quantum signature scheme developed in the CROSSING Collaborative Research Centre that was submitted to the world's first standardisation process in this area. In the implementation of the previous version, the teams were able to identify a cache side channel in the function that generates the signature. By eliminating this weakness, they improved the security of the signature scheme, which could also increase the opportunities in the standardisation process.

In the CROSSING Collaborative Research Centre, a second approach is pursued for evaluating the risks posed by side channels. The researchers take the perspective of an attacker to identify potential side channels experimentally. Hereby, they determine the amount of information about a secret that an attacker can find out at least by a feasible attack. The result indicates how high the danger of such attacks is at least. "The attack-oriented approach allows us to find a so-called lower bound", says Mantel. If the upper and lower bounds lie close together, this confirms the accuracy of the bounds. The security of a system is thus not evaluated absolutely – i.e. not only in terms of "insecure" and "secure" – but rather in more fine-grained degrees of security. This makes it possible to give security guarantees, even for systems that are not fully secure, and to compare the security of such systems. "The question is not only whether a system is secure or not, but a much better question is how secure is a system?", summarises Mantel.

Heiko Mantel views side channels as a promising field for scientific research that is becoming increasingly important in practice: "Spectre and Meltdown constitute two prominent examples of side-channel attacks that were reported widely in the press." Side-channel attacks are very difficult to detect forensically, which is one reason why the Computer Science Professor believes that further research will be beneficial. After you have lost enough money in a poker game, you will realise that something is not going well, and you will try something different or simply stop playing. However, "you do not receive this sort of helpful feedback in the case of side-channel attacks", according to Mantel. "Secrets are revealed but without anybody noticing. And when it does become obvious that somebody knows the secret, it is almost impossible to draw sensible conclusions in retrospect about when, where and how this information was revealed." And this is why the researchers in Darmstadt are continuing to work on giving computers a better poker face.

The author is an online journalist and member of the CYSEC Profile Area.

CROSSING

More than 65 scientists from cryptography, quantum physics, system security and software engineering work together in the CROSSING Collaborative Research Centre at TU Darmstadt and carry out both basic and applied research. The aim is to develop security solutions that will enable the development of secure and trustworthy IT systems even in the future. CROSSING has been funded by the German Research Foundation since 2014.

Weightless research

Many things work in slow motion in space. And researchers at TU Darmstadt are making good use of this fact. Their aim is to investigate the physical process of boiling in more detail.

by Jutta Witte

Cape Canaveral, 25 July 2019: A falcon 9 rocket carrying a Dragon spacecraft takes off for the International Space Station (ISS) at 18:01 local time. Alongside several NASA experiments, the spacecraft is carrying the boiling experiment Rubi (Reference mUltiscale Boiling Investigation) onboard. It was developed by scientists at the Institute for Technical Thermodynamics (TTD) at TU Darmstadt in cooperation with international partners under the umbrella of the European Space Agency (ESA) and was shrunk to the size of a shoe box for its use in outer space. Rubi has now been successfully sending measurement data back to Earth for six months. It is designed to provide insights into which physical processes of boiling, or more precisely the transition phase where a liquid turns into vapour, can be influenced and in what way.

Almost everyone is familiar with this phenomenon from working in the kitchen: When a kettle heats up water for a cup of tea, it firstly starts to simmer: Single bubbles filled with vapour start to form initially at the bottom and then in increasing numbers, rising up to the surface. At 100 degrees Celsius, the water is at full boil and would completely evaporate if the kettle was not switched off. The advantage of the boiling process is that it uses the liquid and also the gaseous phase of a fluid and a lot of energy is transferred during this transition phase. "Boiling is one of the most efficient processes available for transferring energy in the form of heat", explains Axel Sielaff, a scientist at the TTD. It is used, for example, to cool high-performance electronics. Using the measurements taken by Rubi, Sielaff and his team now want to develop more precise models for the heat transfer process.

"Our basic research focuses on the development of products that are not just safer and more compact but most importantly also more efficient."

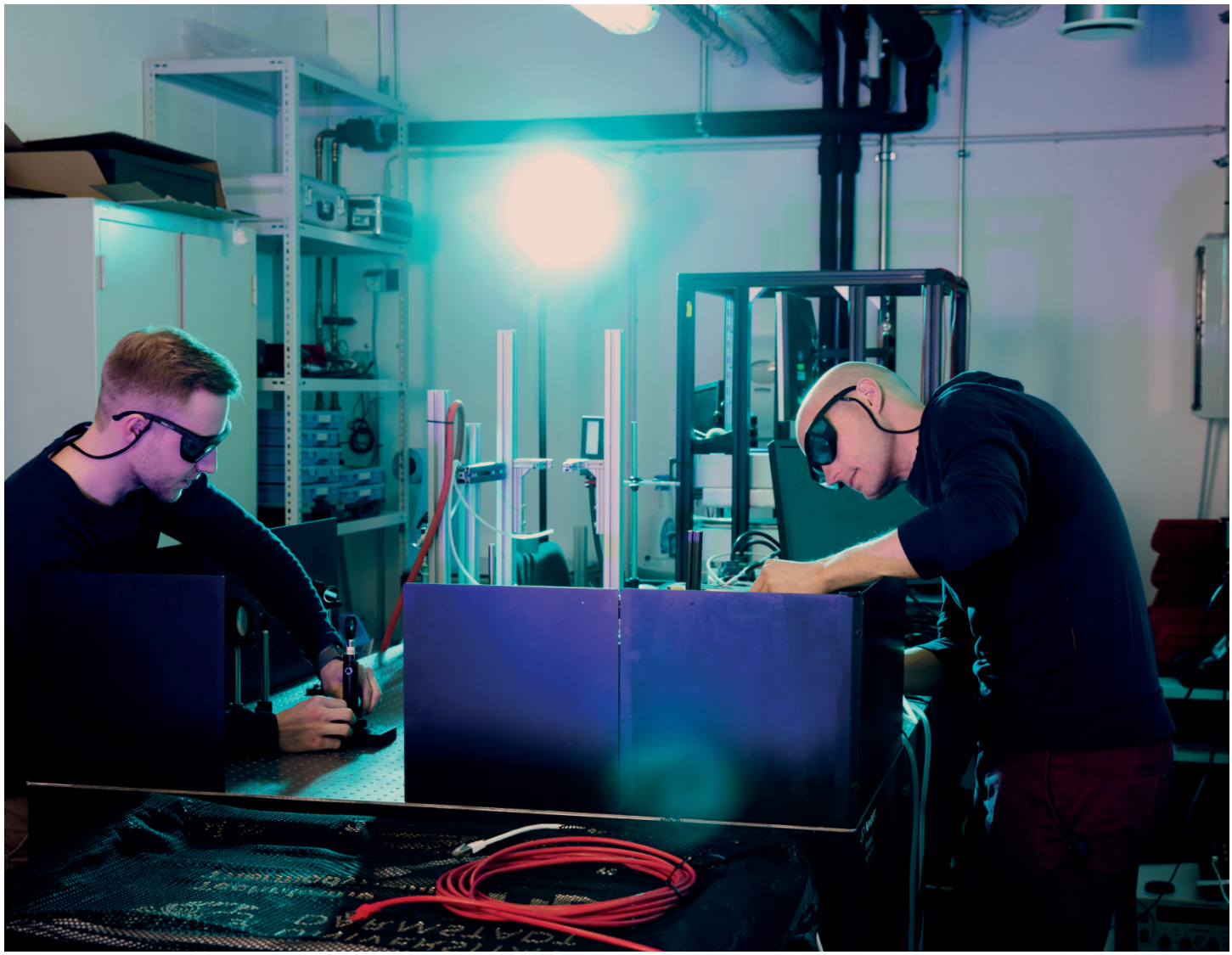
They are conducting research at the interface between mechanical engineering and physics and specialise in everything to do with boiling and evaporation. The current focus of their work are vapour bubbles. "We want to understand the physical phenomenon associated with the creation of vapour bubbles better than has been possible up to now", says the expert. Sielaff boots up the PC in his office at the Lichtwiese Campus and selects one particular experiment from numerous cryptic files. A black-and-white film starts up on the screen. The extremely sharp image shows how a bubble is "ignited" in a controlled manner on a heated surface, slowly grows in size and then comes to a standstill.

What is just a fascinating recording for a layperson, is a source of valuable and detailed information for the experts in thermodynamics. They can analyse the measurement data on the physical properties of the boiling experiments to find out, amongst other things, how much heat can be transferred to a particular point on the surface of the heater, how much energy is expended to create a bubble in the first place, how the temperature in the liquid develops and what influence different combinations of parameters have on the geometry of the bubbles and overall amount of heat transferred.

Information

Institute for Technical Thermodynamics
Dr. Axel Sielaff
Phone: +49(0)6151/16–22272
Email:
sielaff@ttd.tu-darmstadt.de
www.ttd.tu-darmstadt.de

Robin Behle and Dr. Axel Sielaff perform flow field investigations using particle image velocimetry on an identical experimental chamber in the laboratory of the TTD. In contrast to the investigations on board the ISS, the fluid is mixed with small particles and illuminated with a powerful laser. From this, the fluid flows in the experimental cell can be analysed with high temporal and spatial resolution.



Photography: Katrin Binner

These are experiments that are only possible with this level of precision in a weightless environment. This is because processes that happen extremely fast on Earth occur in slow motion on the space station. For example, vapour bubbles form at one single boiling point in a household kettle or in a research laboratory on Earth at a frequency of around 100 per second. In the best case scenario, this figure can be reduced down to zero in space according to Sielaff. This means that the entire development phase for every single vapour bubble can be observed from all possible perspectives and under different framework conditions. What's more, vapour bubbles are only tiny on Earth. In weightlessness, they can reach a diameter of up to ten millimetres.

Making an experiment such as Rubi suitable for use on the ISS and ensuring it runs reliably is no mean feat. During the interview with Sielaff, a technical problem is currently being resolved in Belgium at the User Support and Operations Centre (B-USOC), which controls and monitors Rubi from Earth. Yet Sielaff remains calm. 550 of the 850 experiments that were planned have already been successfully completed at this point in time. This is already considered a triumph. Once this type of experiment has left Earth, the scientists are no longer able to directly intervene in the experiments. After the spacecraft successfully docked with the ISS, Rubi was also connected up manually to the European research module Columbus by the ESA astronaut Luca Parmitano. Control over the experiments was then taken over remotely by the experts at the B-USOC.

"The most difficult issue when developing this type of application for use in space is that it is not possi-

Photography: ESA / NASA

Luca Parmitano is installing the RUBI experiment on board the International Space Station.

Photography: Airbus Defence and Space

The team of Airbus, who built the experiment, is happy about the successful completion.

ble to test the absence of gravity on Earth." For this reason, Sielaff and his team also optimised their experiment in parabolic flights. In order to achieve weightlessness without simply flying into space, this type of flight on a specially equipped Airbus is used to generate alternating phases of 2G and zero gravity – a strenuous workout that the research group completed once a year by flying from Bordeaux out over the Atlantic or Mediterranean. The experimental parameters here are subject to much greater variations than on the ISS. However, the researchers are able to directly influence the experiments on the plane, test different liquids and also quickly change the parameters.

The measurement data recorded during the parabolic flights will be compared with the data generated on the ISS. Sielaff estimates that around 15 to 16 terabytes of data, including around 15 million images, have been transmitted back to Earth from the space station for the Rubi experiment alone since the start of the measurements – firstly via satellite to the base station responsible for the Columbus module in Oberpfaffenhofen and then on to the B-USOC that is responsible for Rubi, where the data that was scrambled in space is recompiled into one file and then sent to the scientists on the core Rubi team in Darmstadt, Pisa and Toulouse for analysis.

Once the measurement phase has been concluded, the evaluation phase begins. The results could be groundbreaking not only for enabling more environmentally friendly cooling and heating of equipment and facilities on Earth, such as computers, data centres, air conditioning systems, batteries or power plants, but also for optimising the thermal regulation systems used in satellites or spacecraft according to Axel. "We want to use our basic research for the development of products that are not just safer and more compact but most importantly also more efficient."

The author is a science writer and holds a doctorate in History.

Photography: Airbus Defence and Space

Before the experiment is allowed to enter the ISS, it is tested in a replica of the Fluid Science Laboratory at B-USOC in Brussels. An identical experiment will remain there for reference investigations.

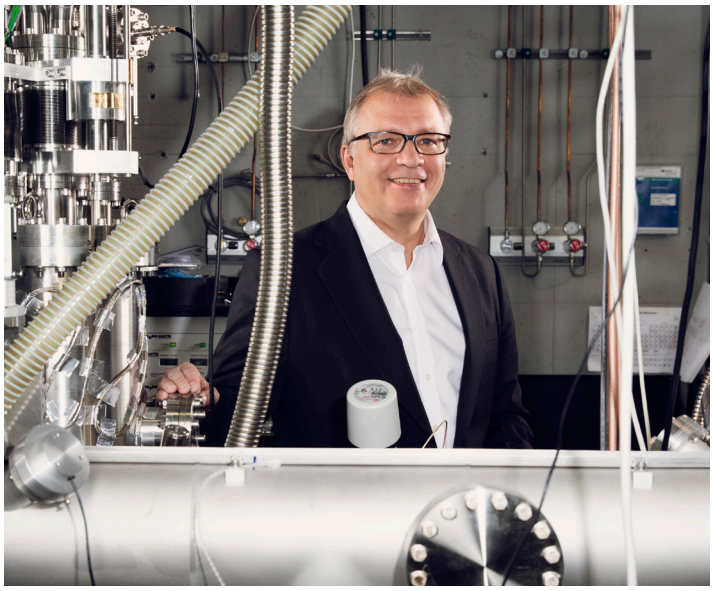
The Experiment

The boiling experiment Rubi (Reference mUltiscale Boiling Investigation) is part of the Fluid Science Laboratory (FSL) in the European ISS research module Columbus. A heater that was developed and built in Darmstadt heats up a coolant. A laser "ignites" single bubbles at a defined location. A high-speed camera captures the entire development of this bubble, while an infrared camera measures the heated region. Rubi also contains a pump to generate a shear flow, meaning that the liquid continuously flows over the heated surface from one side. High voltage can also be generated in the experimental space using an electrode to investigate the influence of an electric field on the development of the bubbles. The experiments are saved on the ISS but can also be followed live from Earth.

The Consortium

Under the coordination of Prof. Dr.-Ing. Peter Stephan, Head of the Institute for Technical Thermodynamics (TTD) at TU Darmstadt, 14 universities and research institutions from Europe, Russia, Japan and the USA are participating in Rubi, including the Department of Energy, Process and System Engineering at the University of PISA, the "Institut de Mécanique des Fluides de Toulouse" (IMFT) and the Multiphase Dynamics Group at the Aristotle University of Thessaloniki. The experiment was financed by the European Space Agency (ESA), jointly developed with Airbus Defence & Space and is controlled by the Belgian User Support and Operations Centre (B-USOC). In order to share and jointly optimise the evaluation methods developed as part of Rubi, the TTD initiated the programme "Code exchAnge for Rubi Analysis Tools" (CARAT) which can be accessed by all research partners. Rubi is part of the Thermo-Fluids & Interfaces Profile Area at TU Darmstadt.

Signposts for tiny lightning strikes



Photography: Katrin Binner

Professor Lambert Alff is a materials scientist. He carries out research and teaches in the field of electronic materials and thin films.

Researchers in Darmstadt are developing memory devices for a new type of chip.

by Christian J. Meier

Lambert Alff controls lightning bolts, although only on a microscopically small scale. The professor aims to use these discharges to produce memory devices for computers that can also process data at the same time. "This is the next revolution in computer technology", says Alff. He recently made and published an important contribution to this research with his team in the Materials Science Faculty at TU Darmstadt, in cooperation with the group headed by Dr. Leopoldo Molina-Luna who are carrying out research just a few doors down the corridor.

What does the materials scientist mean when he talks of a revolution? The "Internet of Things" is becoming more tangible every day. An increasing number of everyday objects contain small computers and these smart objects now often transmit the data to the cloud where it is processed. This transmission process requires energy. In addition, processors need to be constantly supplied with energy because otherwise they will lose data. "In twenty years' time, the IT sector alone will require as much energy as is consumed today in total around the world unless we develop something new", warns Alff.

Information

Materials Science
Prof. Dr. Lambert Alff
Phone: +49(0)6151/16–20700
Email:
lambert.alff@tu-darmstadt.de
www.mawi.tu-darmstadt.de/ds

Alff has a clear vision of what this new development will look like: Non-volatile memory modules that can also process data at the same time. After being switched off, the chip will save its current status like a paused film and continue to process the data as soon as the power supply is restored. "A smartwatch could thus record jogging data and also process it by itself", says Alff. The researchers in Darmstadt had an eye on the future application of this technology from the very beginning, which is why they are developing their components based on hafnium oxide, a material that is already used in the production of chips today. The team uses tiny crystals of this substance that are smaller than a virus. The crystals do not conduct electricity. However, if you apply an increasing amount of voltage to them, there is eventually a discharge: A channel opens up in the crystal, through which electrical charge can now flow. This channel can be closed again and the element thus behaves like a switch that can save its current state even without a power supply. And this is precisely what is required.

However, the individual components have to be switched at different voltages up to now and are thus not suitable for use in the electronics sector. "We are now demonstrating how it is possible to develop components with less variability", says Alff. Alff attributes this success to the cooperation with Molina-Luna. "I am delighted that we have two teams here in Darmstadt that complement each other so well for this type of research." The group headed by Molina-Luna are investigating the components produced by Alff's team using an electron microscope. This has allowed the researchers to identify the important role played by so-called grain boundaries. Each component consists of multiple tiny grains of crystal, just like a 3D mosaic. The discharges run along the boundary edges between the grains. Normally, there is not much order to the structure of the "mosaic". The researchers thus deposit layers of hafnium oxide onto an electrode, whose crystal lattice had a particular orientation. The grain boundaries in the hafnium oxide took on this orientation and became much more ordered as a result, especially with respect to the shortest route between the switching contacts. The lightning bolts are thus offered a much clearer path and the switching voltage does not fluctuate as much.

As a next step, the group now aims to precisely determine the location where a grain boundary will grow so as to reduce the variability even further. "For this purpose, we want to give the base plate on which the crystals grow a defined structure", says Alff. This could be a tiny groove along which the grains orientate themselves. If Alff and Molina-Luna continue to work so well together, they are sure to succeed.

The author is a science writer and holds a doctorate in Physics.

Publication:

Stefan Petzold, et al: *Forming-Free Grain Boundary Engineered Hafnium Oxide Resistive Random Access Memory Devices,* Adv. Electron. Mater. 2019, 5, 1900484.
https://doi.org/10.1002/aelm.201900484

Professor Lambert Alff presents his work on YouTube
https://www.youtube.com/watch?v=us8pjhG8ve0