hoch3 FORSCHEN

SCIENCE QUARTERLY

Spring 2017

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)

Conceptual design
conclouso GmbH & Co. KG, Mainz, Germany

Photography (title)
Katrin Binner

Circulation
6.000

Next issue
15th of June 2017

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

Eavesdrop resistant into the future

The TLS 1.3 protocol will provide the Internet with a new standard for encrypted communications. Led by Professor Marc Fischlin, a team of researchers at the TU Darmstadt collaborated in the analysis of the protocol and tested its cryptographic processes. These are more efficient and less error prone, but are they future proof?

By Boris Hänßler

Heartbleed, Triple Handshake, Crime – these cryptic-sounding names all refer to attacks on one of the core elements of the modern Internet: the Transport Layer Security (TLS) protocol for encrypted communications. We all use it to protect our data whenever we google something, buy from online shops or send an email. Generally speaking, we can rely on the TLS protocol: the worst hacker attacks carried out in the last few years were all the result of failures to properly implement it. Nevertheless, many experts were still unhappy with the protocol. On the one hand, researchers themselves have periodically been discovering minor security breaches in the protocol itself. On the other hand, many Internet-based companies have been finding the protocol too cumbersome and not fast enough.

That's why the international "Internet Engineering Task Force" (IETF) has introduced a new protocol known as TLS 1.3. Together with his team, Marc Fischlin, Professor of Computer Sciences at the TU Darmstadt, used their expertise in cryptography to carry out an analysis of the new standard. During the development process, which spanned several years, they tested the proposed procedures and their new functions to ensure that they really are sufficiently secure and that they will be able to keep pace with future technological developments.

"The reduction of round trips is among the most important innovations, but also entails certain risks."

One security risk that Fischlin's team has been looking into is the result of fewer so-called "round trips" in the new protocol. To establish a TLS connection, the client – for example the PC used by a customer of an online shop – and the shop server negotiate an encryption key in several steps. The contact is initiated by the customer's PC, which essentially says: "Hello. I'd like to communicate with you and propose the following encryption keys." The server then selects one of the available encryption keys and simultaneously transmits an official authentication certificate, which confirms that it really is the server of the shop in questions. The customer's PC accepts the key in turn and, following a number of additional steps, both parties declare the negotiation processes to be complete. Only then can the actual data exchange take place. This technical dialogue consists of six steps in total. One objective of the new protocol was to reduce this negotiation process to just four steps, which the developers succeeded in doing by combining two formerly separate processes.

If the client and server already know one another, for example because the customer has already bought things from the online shop, then the new TLS protocol permits them to communicate immediately. Computer scientists refer to this as a "zero-round-trip-process" because no additional encryption key negotiation rounds are required. The customer's PC authenticates itself using a so-called "session ticket", which it receives and saves during the initial encryption negations upon first contact. It can use the ticket to transfer its relevant data.

The reduced number of round trips is not something that we would notice in our everyday Internet usage. Even the old version of the protocol was so fast that its impact on our communication speeds was negligible. However, the situation is entirely different for search engines such as Google, which, at the last count, registered some two billion search queries per year. Every time someone reloads the search engine in their browsers, a new encryption key has to be negotiated. Therefore, the round trip reduction in the updated protocol represents a significant traffic load reduction for companies such as Google. "Without doubt" Fischlin explains, "this is one of the most important innovations of TLS 1.3. But it does involve certain risks".

One of these risks is the subject of a current research project, which Fischlin and his team will be presenting at the 2nd IEEE European Symposium on Security and Privacy in Paris in April. The subject of the study are

Information

Institute of Computer Sciences and Complex Cryptography
Prof. Dr. Marc Fischlin
marc.fischlin@cryptoplexity.de
http://bit.ly/2mlTbs9

so-called “replay attacks” in zero round-trip scenarios. In the course of such an attack, the hacker would attempt to intercept the session ticket. Whilst he or she would not be able to use it to read or alter the transmitted data, they could use it to send multiple requests to a given server. If, for example, a user were to order a book from an online retailer, the hacker would be able to reorder the book thousands of times at the user’s expense.

For this reason, the TLS 1.3 protocol should enable online shops and other service providers to check if user requests are repeats of earlier requests; whether, for example, the same product is being ordered multiple times. If so, then the session ticket will be invalidated, and the server and client would have to negotiate a new encryption key, thus taking the would be hacker out of the loop. Fischlin and his team were able to prove that the new protocol meets the new security requirements even in the face of any conceivable exceptional case. “There are still residual risks involved”, says Fischlin, “but we consider them to be so minuscule that we consider the new protocol to be robust”.

The Darmstadt researchers are also looking ahead to future functions for TLS 1.3. Anti virus software manufacturers, for example, would like it if their software could search encrypted data, instead of having to wait until the files are decrypted. “We’re working on procedures that would enable this”, says Fischlin: “One option, for instance, would be to carry out computations directly on the encrypted data string. The virus scanners would be able to recognise damaged or compromised code based on the encryption pattern. Of course, we’d have to ensure that standardised information included in the files, such as banking data, could be read out using the same method.”

In the distant future, cryptography experts will be faced with another problem if quantum computers are ever realised, which would render current encryption processes, based on the so-called Diffie–Hellman key exchange method, obsolete. This process is deemed secure because it is based on a mathematical problem that is fundamentally intractable for current computers. Quantum computers, by contrast, could solve it. As Fischer explains: “No one can say whether such computers will ever be realised. But, as soon as they are available, all these procedures would become obsolete overnight. We need to be prepared for this.”

One potential replacement would be the so-called learning with errors problem (LWE), which, it is assumed, could not be solved by quantum computers. So why isn’t it being used already? “Ah”, Fischlin explains with a grin, “that would increase protocol latency again, which just goes to show that cryptographers are not going to run out of research subjects any time soon!”

The author is a science writer.

Photo: Katrin Binner

Carrying out research into cryptography, security and complexity theory: Professor Marc Fischlin (ed.)

Clean carbon capture technology

In the course of Project SCARLET, scientists at the TU Darmstadt have succeeded in developing the so-called Carbonate Looping process for the reduction of CO_2 emissions during power plant operations almost to the point of market readiness.

Jochen Hilz, Dr.-Ing. Jochen Ströhle, Prof. Dr.-Ing. Bernd Epple (from left to right) in the CO_2 testing facility at the Institute for Energy Systems and Technology (EST), which houses the 1 MW experimental pilot plant.

By Hildegard Kaulen

By the time Professor Bernd Epple of the TU Darmstadt's Institute for Energy Systems and Energy Technology opens the final symposium of the European-wide Project SCARLET these coming days, several milestones will have been reached. Over the past three years, Professor Epple, a mechanical engineer, and his ten German and international project partners have developed the technical prerequisites for the industrial deployment of the Carbonate Looping process. This process can be used to separate more than 90 per cent of the CO_2 released during the combustion of fossil fuels. Retrofitting existing power generation facilities and industrial plants with this technology would allow them to be operated in a much more environmentally-friendly manner.

Based on data measured at a 1 Megawatt (MW) experimental facility, Professor Epple and his team have developed scaling tools for industrial plants with which they have conducted model calculations and computer simulations. They have proven that the new process is more cost effective and energy efficient than competing processes. They presented plans for a complete pilot project plant for the coal-fired power plant Émile Huchet in Saint-Avold in France, with a total output of 20 MW. "If the funding details were already clarified at this point", says Dr. Jochen Ströhle, Senior Research Scientist at the Institute for Energy Systems and Technology at the TU Darmstadt and Project SCARLET coordinator, "then this could be the first industrial scale pilot project to be launched. "All the necessary planning, including a cost schedule and a risk assessment are already on the table". The acronym "SCARLET" stands for "Scale up of Calcium Carbonate Looping Technology for Efficient CO_2 Capture from Power and Industrial Plants". The European Union has provided five million euro in project funding, and the overall budget was over seven million euro.

How does the carbonate looping process work? Carbonate Looping involves two chemical reactions continuously running in two interconnected fluidized bed reactors. In the first fluidized bed reactor, the absorber, a powder of burnt lime or calcium oxide (CaO) is contacted with the CO_2 in the power station exhaust to form calcium carbonate ($CaCO_3$). The calcium carbonate then is transferred in the second of the two fluidized bed reactors, known as the regenerator, where high temperatures force out the CO_2 bound as the calcium carbonate thereby producing burnt lime and CO_2 once again. The released CO_2 can then be used for other purposes or stored whilst the burnt lime is returned to the first fluidized bed reactor. The material needs to be replaced after several dozen cycles, but the depleted lime can then be used in cement production making it a valuable raw material rather than a waste product.

"We need 80 kilograms of lime to capture one tonne of CO_2", Professor Epple explains. "The current process costs amount to around 20 to 27 euro per tonne of CO_2. Other processes are more expensive and

Information

Institute for Energy Systems and Energy Technology
Prof. Dr.-Ing. Bernd Epple
Phone: ++49 (0)6151/16–23002
bernd.epple@est.tu-darmstadt.de
www.est.tu-darmstadt.de

less efficient. Through SCARLET we have succeeded in moving the Carbonate Looping process a major step forward towards market readiness". What did the project partners do in particular? First, it was necessary to discover the conditions and prerequisites for the continuous operation of the 1 MW pilot plant within grounds of the TU Darmstadt. Only under stable operating conditions it is possible to extrapolate from the measured data to calculate the necessary scaling factors. The pilot plant was built six years ago with funding from the German Federal Ministry for Economic Affairs, the European Union, and various industrial partners. "Today, we operate the 1 MW facility for several weeks at a time with a constant level of CO_2 sequestration", explains Jochen Hilz, a doctoral candidate who has been supporting the project right from the outset. "The reactivity of the lime declines as the number of cycles increases, which necessitates operating periods lasting up to several days, to be able to draw reliable conclusions to its long-term behaviour. We now know the conditions necessary for steady operations. The more empirical data we have from continuous operations, the fewer assumptions we need to make and the better are models and computer simulations that we calculate."

"Next, we're planning a facility that will separate out the CO_2 that is generated during waste incineration."

For SCARLET, it was necessary to upgrade the 1 MW experimental facility. "For example, we built a silo for 30 tonnes of fuel", Professor Epple reports, who developed the concepts for the process based on his professional work for an industrial corporation. "You see, we need a constant supply for continuous operation. We also had to improve the transfer of particles from one fluidized bed reactor to the other in addition to adapting existing measurement systems. What we wanted to know was how the particles move inside the fluidized bed reactors; their relative densities in various zones, and what velocities they can achieve. Also", Epple continues, "we wanted to analyse the gas at the different levels. That's the only way we can understand how fast the CO_2 has been separated in the absorberand then set free again in the regenerator". Because temperatures of 900 degree Celsius are reached within the fluidized bed reactors, measuring this data is anything but trivial. "Basically", Epple explains, the "reactor contents are like molten lava".

It was not easy to measure what actually happens within the reactors during the Carbonate Looping process. As Dr. Ströhle explains: "We knew how the process behaves in general, and that high CO_2 absorption efficiencies are possible. On the other hand though, we knew very little about the long-term behaviour of the lime under real operating conditions. That has now changed following SCARLET." This knowledge was used in collaboration with the project partners to develop models for larger facilities and various plant types. The process can also be used for industrial cement and steel plants as well as waste incineration facilities.

So, what's next? "We'll be taking various approaches" says Professor Epple, "Including, for example, planning a facility that separates out the CO_2 produced during waste incineration." The project team is also discussing concepts for the utilization of the recovered CO_2. The price per tonne of CO_2 is currently very low on the global markets. At this point, any power plant operators making use of the process would not be in a position to be able to sell the captured CO_2 at a rate that would enable them to break even, let alone make a profit. It would have to be stored or reprocessed. "We're considering using the CO_2 directly for the production of methanol", says Professor Epple. "Global market prices for methanol are higher than those for CO_2." He and his team have developed the process even further to the point where pure oxygen will no longer be required for combustion within the regenerator and the overall efficiency level will be increased. They are determined to bring the project to a successful conclusion.

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

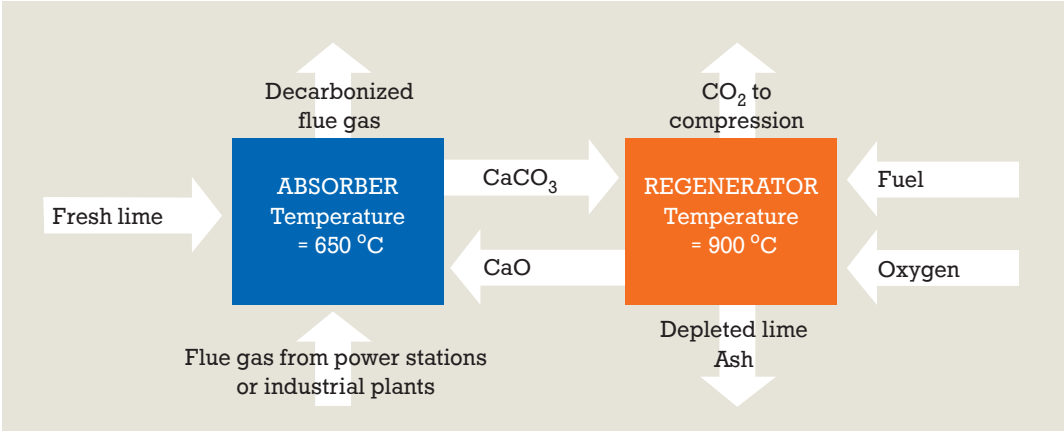


Table: Prof. Dr.-Ing. Bernd Epple; Design: Ulrike Albrecht

Imprinting with d

Materials scientists at the TU Darmstadt are imprinting nano-patterns in metals, a technology that could give metallic surfaces permanent functionality, like a lotus effect or reduced frictional properties.

By Uta Neubauer

A baker specialising in the spiced Spekulatius biscuits eaten in Germany around Christmas time and Paul Braun, a doctoral student at the Physical Metallurgy group in the Department of Materials and Earth Sciences at the TU Darmstadt have one thing in common: they both spend some of their time imprinting designs into materials – the one into biscuit dough; the other into metal. However, whilst the animals, figures, and windmills typically stamped into the Christmas cookies are readily identifiable, Braun's imprints are too small to be invisible by the naked eye. They are formed into the metal using a tiny stamp made of diamond no bigger than the point of a needle. "Diamond is perfect for the task", Braun explains, "as it is an extremely hard material that is all but impervious to wear and tear."

"When punching or stamping metal, it would be possible to mould the surface at the same time to introduce specific functionalities."

To be able to be used for embossing, the diamond is clamped in a special device, a so called nanoindenter. Actually, the materials scientists at the TU Darmstadt usually use the nanoindenter for complete different purposes, such as testing the hardness, fracture behaviour, and other properties of various materials. These tests all involve the use of a diamond stylus that is pressed into the material being tested, whereby a force is applied and the indentation depth is measured on the nanoscale. In addition, the device can be used in combination with a scanning electron microscope (SEM) to study cracking of thin coatings during the indentation process. Braun's doctoral supervisor Dr. Karsten Durst, Professor of Physical Metallurgy at the TU Darmstadt, explains: "The diamond tip is pressed less than 100 nanometres into the sample during such tests, so that the nanoindenter can be used to explore gossamer-thin layers." For many years he has been driving the development of this method for materials testing purposes and is now using it to address novel problems. He now plans to use it for the nano-scale imprinting of metal surfaces. This technology, which experts refer to as nano-imprinting, is already being used in conjunction with polymers, for example in the manufacture of plastic chips which include microscopic channels and other structures. Nor is the embossing or imprinting of metal anything new in principle, but it has only ever been used at far larger scales to date for things such as minting coins. According to Durst: "We're right at the beginning of the nano-imprinting of metallic surfaces, and are still looking at the basic principles of this technology".

Information

Physical Metallurgy Group (PhM)
Prof. Dr.-Ing. Karsten Durst
Phone: ++49(0)6151/16–20551
k.durst@phm.tu-darmstadt.de
http://bit.ly/2mchYzt

The first step is the development of suitably hard and finely structured stamps. Doctoral student Braun has already succeeded in creating several of these by re-purposing the diamond tips of a nano-indenter, to which end he travelled to Brno in the Czech Republic to meet with the microscope manufacturer Tescan, who have developed a special ion beam technology. This is usually used for the preparation of samples for examination by electron microscopy. Braun, on the other hand, used the focused ion beam to cut off the top of the diamond probe, to carve a pillar out of the remains of the diamond, and to mill the desired pattern into its top surface. After final ion beam polishing, the stamp was ready for use.

The next question is: what properties does a piece of metal need to have so that it precisely forms the desired surface structure. As every Spekulatius baker knows, the success of the biscuit depends on the consistency of the dough. The same applies, in principle, to the nano-imprinting process: the microstructure of the metal has to be just right to ensure that it "flows" well into the mould. The scientists in Darmstadt want to be able to imprint structures of just 50 nanometres – that's around 1500 times thinner than a human hair! The problem: any metal or alloy will consist of a multitude of tiny, tightly packed grains. For most conventional metals and alloys the diameter of these grains measure well above 1000 nanometres. This means, however, that conventional grain sized metals will resist being pressed into the form of the stamp due to their large grain size. This is why Durst and his colleagues are researching the production of more finely-grained metals, which will fit perfectly within the hollow spaces of the stamps.

Such nano-crystalline metals can, for example, be produced by means of a galvanic deposition in conjunction with special additives or through the so-called severe plastic deformation process. There are several variants of this latter technology including the high-pressure torsion process used by Durst and his team. This involves twisting a piece of metal in a tool, which at the same time exerts a high pressure. This high-pressure torsion process causes a large shear deformation, which in turn kneads the metal making it more finely grained.

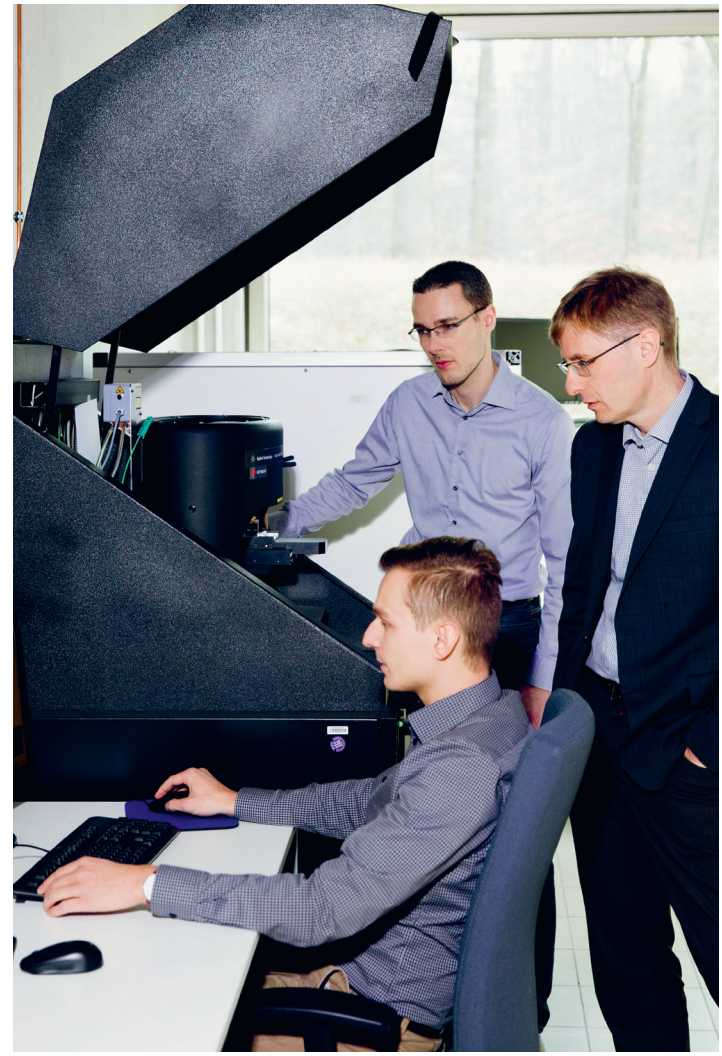
Research into nano-crystalline materials and their deformation-related structural changes is being carried out by Dr. Enrico Bruder, a member of Durst's group. Bruder is using an SEM to image the ways in which the crystalline structures become smaller and reorient themselves during the deformation process. Not only is this structural change of interest in the context of the imprinting process, it also results in the

liamonds

emergence of novel properties as Durst emphasises: “Nano-crystalline metals are usually strong, but they still can be shaped with other forming processes, without failing in a brittle manner”. Which, of course, are the best possible properties for nano-imprinting.

Albeit Durst and Braun both emphasise the fact that they are still a long way from an industrial realisation of this technology, they do have a number of applications in mind. For example, one could emboss a metallic surface with the same nano-structures found on the leaves of lotus plants, from which water droplets simply roll off taking any impurities with them. It may also be possible to engrave tiny lubricant reservoirs into metal components. The nice thing about nano-imprinting, according to Durst, is that the technology could be integrated into a continuous manufacturing process: “Whenever metal is rolled out or stamped out”, he explains, “it would be possible to emboss the surface at the same time to introduce specific functionalities.” The imprinting process could be used, he goes on to emphasise, to create much finer structures than are possible with lasers. One can readily imagine tool arrays consisting of multiple rather than single stamps as well as the corresponding roller presses. Actually, German Spekulatius bakers have already invented all of these things, and they work wonderfully well.

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



Materials scientists deep in concentration: Dr. Enrico Bruder, doctoral candidate Paul Braun and Prof. Dr. Karsten Durst (from left to right to right).

Photo: Katrin Binner

New research device approved

In the course of the “New Systems for Fundamental Research” call for proposals, the German Research Foundation (DFG) approved twelve out of a total of 79 applications in December 2016. One award went to the Physical Metallurgy Group in the Materials Science Department at the TU Darmstadt, where Professor Dr. Karsten Durst and his team will be able to use the three-year project funding to progress the development of a nano-indenter for high-temperature materials testing. The researchers are planning to use the newly developed systems for analysing materials used in turbine engines and other applications that need to withstand extremely high temperatures. The objective are readings in the range of > 1000 degrees Celsius. The TU Darmstadt is already home to three nano-indenters capable of recording temperatures of up to 500 degrees Celsius.

More and more materials comprise either nano-structures or are nano-coated. Performing realistic analyses of these materials will require the use of new equipment such as the nano-indenter that has now been approved but which is not available “off-the-shelf”. One problem is that the diamond tip, which is pressed into the surface to be measured, would burn up if exposed to air at the extremely high temperatures involved. The analysis must therefore be carried out in a vacuum chamber. Alternatives to diamonds are also being tested. The extremely precise positioning of the tip, which is a prerequisite for nano-scale measurements, also represents a challenge in the high-temperature range. “The procurement of the high-temperature nano-indenter is a development project”, says Durst. The initial concepts for this are currently being drafted.

Publications:

K Durst, V Maier: Dynamic nanoindentation testing for studying thermally activated processes from single to nano-crystalline metals. **http://bit.ly/2mZqGoj**

V. Maier, C. Schunk, M. Göken, K. Durst 2015): Microstructure-dependent deformation behaviour of bcc-metals–indentation size effect and strain rate sensitivity. **http://bit.ly/2mPzn4m**

H. ur Rehman, K. Durst, S. Neumeier, AB. Parsa, A. Kostka, G. Eggeler, M. Göken (2015): Nanoindentation studies of the mechanical properties of the μ phase in a creep deformed Re containing nickel-based superalloy. **http://bit.ly/2lLdO59**

Pieces of Cosmic Puzzles

They conduct research into extremely exotic atomic nuclei, to achieve a better understanding of the emergence of heavy elements, and scientists at the TU Darmstadt have now found an explanation for the brief existence of the so-called tetraneutron. They have also discovered clues that may help to solve an important puzzle concerning neutron stars.

By Christian Meier

Robert Roth decided to study physics because he was fascinated by astronomy, which focuses on the extremely large: stars, galaxies, and the universe. Today, as a professor at the Institute for Nuclear Physics at the TU Darmstadt, his research concerns the extremely small: atomic nuclei and their building blocks. He is particularly interested in extremely exotic nuclei about which he and his team have published two works in collaboration with researchers from Russia and the USA.

The extremely large and the extremely small According to Roth, there is no contradiction involved. On the contrary: an understanding of each of these areas is a precondition for an understanding of the other. Stars, for instance, are the nurseries of atomic nuclei and, therefore, of the elements. On the other hand, the life of a star is influenced by the properties of atomic nuclei.

There is still a lot to learn: As the theoretical physicist explains: "We still don't know how the gold that many people wear on their ring fingers came into existence." What we do know is that atomic nuclei are forged in the centres of stars through so-called nuclear fusion processes, during which protons and neutrons are melded together. Yet elements that are heavier than iron, such as lead and gold, cannot be formed in this way.

Only catastrophic events, such as supernovae or collisions of so-called neutron stars can create the necessary conditions. "These events release large quantities of neutrons", Roth explains. These serve as the raw ingredients for the formation of heavy atomic nuclei that grow through the capture of many neutrons within fractions of milliseconds. If these capture processes occur too slowly then the non-stable interim products decay before heavy atomic nuclei such as lead or gold are reached. "What we need to know", says the physicist, "is how neutrons interact with one another under such extreme conditions."

His Darmstadt team are breaking new ground, for example, by using the Lichtenberg supercomputer at the TU Darmstadt to simulate highly exotic nuclei such as the "tetraneutron", which consists of just four neutrons. An object such as this ought to disintegrate immediately, because the attractive force between neutrons is extremely weak. However, recent experiments have hinted that tetraneutrons do exist for short periods. "Our calculations provide a possible explanation for this" says Roth. For the first time ever, the researchers have taken the decay of the tetraneutron into account in connection with quantum-theoretical approaches used to describe these systems, which are already complex enough. In this way, they discovered that the four neutrons form a so-called resonance for an unimaginably short time (a billionth of a billionth of a ten-thousandths of a second). "Which", Roth concludes, "means that the tetraneutron can actually exist!" These studies will continue in the context of the Collaborative Research Centre 1245, which is funded by the German Research Foundation, and will include new experiments carried out in Japan by the experimental group around Professor Thomas Aumann that aim to prove the existence of the tetraneutron resonance beyond doubt.

In the meantime, Roth's team are researching even more exotic atomic nuclei, which include so-called hyperons in addition to neutrons and protons, which is why they are referred to as hypernuclei. Hyperons include a so-called strange quark, whereas protons and neutrons do not. "We have discovered clues that contribute to solving the so-called hyperon puzzle", says Roth, the "puzzle" being that hyperons ought to form in neutron stars, which can have twice the mass of our sun; yet, if they did, then such heavy neutron stars could not exist ... but they do!

It may well be that Robert Roth and his team will succeed in solving one of the mysteries of these celestial objects by gaining a better understanding of their tiniest building blocks.

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

Publications: Shirokov, A.M. et al: Physical Review Letters, 117, 182502 (2016). Wirth, R., Roth, R.: Physical Review Letters, 117, 182501 (2016).

Photo: Katrin Binner

Professor of Physics Robert Roth

Information

Institute for Nuclear Physics – Theory Centre
Prof. Dr. Robert Roth
Phone: ++49(0)6151/16–21540
robert.roth@physik.tu-darmstadt.de
http://bit.ly/2lLl14i