hoch3 FORSCHEN

SCIENCE QUARTERLY

Autumn 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)

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

Title Simplified diagnostic methods are developed in the Merck Lab at TU Darmstadt

Photography (title)
Katrin Binner

Druck Druckerei Petzold, Darmstadt
printed oh 100 g/m² PlanoScript, FSC-certificated

Circulation
5.000

Next issue
15th of December 2020

Service for readers
presse@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

Computer science for peace

He is conducting research and teaches on the interface between computer science and peace and conflict research. Professor Christian Reuter explains in the following interview how IT can be used during war and to bring about peace.

Photo: Hessen schafft Wissen – Jürgen Kneifel

Professor Christian Reuter

Professor Reuter, the Council of Science and Humanities is calling for the further structural development of scientific and technical peace and conflict research in Germany. How well prepared are we here in this respect?

We are clearly less well prepared in comparison to peace and conflict research in the political sciences. Greater importance was placed on this field in the past. Scientists were already focussing on dual use issues back in the 1950s and 1960s and thus considering, for example, how they could help to ensure that nuclear power was only used for supplying energy and not also for producing weapons-grade materials. Today, this type of research is underrepresented at German universities. From a structural perspective, this research is currently only permanently carried out at the Carl Friedrich von Weizsäcker-Centre at the University of Hamburg and here at TU Darmstadt. Yet these topics are more current than ever. We should by no means think that things have become more peaceful everywhere. On the contrary, chemical weapons are being used in Syria and international treaties on the disarmament of long-range missiles have just been terminated. Certainly, we are also faced with totally new challenges in cyberspace.

What role do cyberwarfare and cyber forces play nowadays?

Harmful activities taking place between countries in cyberspace are now the norm and cyber forces have become a new pillar of warfare alongside land, air and sea forces, and activities being carried out in space. Many countries and alliances are building up their cyber capacities. This is true for the USA and also for NATO as well as individual countries such as Germany. Money and resources are being invested in this area everywhere and new units and powers are being build up.

What is a cyberweapon exactly?

It is certainly nothing like what we are familiar with from the Star Wars films. The whole situation is much more subtle. Usually, it involves security vulnerabilities in software and hardware combined with code to exploit them. These vulnerabilities are becoming an increasingly valuable commodity. If you want to misuse them for military conflict, you don't notify the manufacturers about them but collect them in your own weapons arsenal. If you have exclusive knowledge about these types of backdoors, you have a decisive advantage for influencing the outcome of a war. Anyone who has been active in cyberspace for a long time can use this knowledge to penetrate IT systems operated by the enemy. This poses a threat not just to military systems but also to civil ones – if, for example, not only the missile base but also an energy supply system becomes the target.

Is it possible to track these types of hostile activities?

In general, we are unable to track them. If somebody launches a rocket, it can be seen on satellite images. However, it has still not been possible to fully understand and trace the hacker attack on the German government in December 2017. It is often not even possible to determine whether these attacks are simply criminal activities or espionage – which although they can be prosecuted under criminal law, would not trigger a war – or whether in cooperation with transnational players they are really intended to provoke a conflict between nations. The whole situation is a little blurred. We are seeing a dangerous normalisation of constant harmful attacks and hybrid conflicts. And this is not exactly promoting trust between countries.

Contact

Science and Technology for Peace and Security (PEASEC)
Prof. Dr. Christian Reuter
Phone +49(0)6151/16 – 20941
E-mail:
reuter@peasec.tu-darmstadt.de
https://peasec.de

Photo: shock/stock.adobe.com

Amongst other things, the PEASEC is carrying out research into resilient IT-based critical infrastructures.

You have raised the subject of dual use technology. What can you do in computer science to ensure that new, digital technologies are not misused in warfare?

This is not only about assessing the impact of technology or safeguarding infrastructures but importantly also about the conscious design of technology. We need to develop software right from the very beginning that is designed to provide as few opportunities as possible for misuse or use in conflict. However, the dual use problem represents a huge challenge especially in the area of information technology. It is still possible to change software relatively easily and adapt it for purposes other than its originally intended use.

In your institute, computer scientists work together with peace and conflict researchers. How does this work in practice?

Our research is carried out in areas where these two disciplines overlap. On the one hand, we utilise the methods of empirical social research and analyse, for example, the role of new technologies for peace and security. We examine questions such as: How is social media used in conflict situations? What dynamics are created there as a result? What narratives are used to manipulate opinions? We then develop technical solutions on this basis to prevent escalations such as so-called information warfare. For example, we have developed a plug-in for browsers called "Trusty Tweet" that flags up indicators of fake news. We are also working on software that analyses social media data to prevent misuse, such as the tracking of persons, from the outset.

I would imagine that this type of continuous, interdisciplinary cooperation is very demanding.

Yes. It presupposes that researchers can develop a deep understanding for the other field of research. But that's not all. We have to get to the very heart of the issues together so that we clearly understand which specific points we want to focus on. The process does not begin by focussing on the technical issues. The starting point is always a deficit that has to be analysed in more detail in order to develop possible technical solutions for the benefit of society. At the same time, we also have to gain acceptance in our own relevant specialist fields. This is because we want to be able to introduce our findings into the individual disciplines at the very highest level so that our research becomes visible and others are able to build on it. This usually requires us to go the extra mile once again.

What is it that you would like to achieve in your own specialist field?

As computer scientists, we have a practical influence in this day and age on the whole of life. I would thus like to raise awareness for the fact that our work can also cause damage and we have to place more focus on value-based design in which not only monetary aspects play a role. Software can often result in unintentional developments in the wrong direction. Therefore, we have to learn to actively make decisions and already set the right course during the software development phase so that we can, for example, exclude certain types of use of the software or only provide certain modules in encrypted form. Everyone of us should become aware of these issues.

The interview was conducted by Jutta Witte.
She is a scientific journalist and history graduate.

Background:

Prof. Dr. Christian Reuter is head of the research group of Science and Technology for Peace and Security (PEASEC) at TU Darmstadt that was established in 2017. He is a member of the Department of Computer Science and is also affiliated to the Department of History and Social Sciences. The PEASEC team carries out research into the themes of "Safety-Critical Human-Computer Interaction", "Information Technology for Peace and Security" and "Resilient IT-based (Critical) Infrastructures". The group is closely intertwined with the cybersecurity profile area at TU Darmstadt (CYSEC) and the multi and interdisciplinary network IANUS in the Forum for Interdisciplinary Research (FiF) at TU Darmstadt.

https://peasec.de/2020/it-frieden

Latest publication:
"Towards IT Peace Research": https://peasec.de/2020/towards-it-peace-research

Diagnostics from a printer

At the Merck Lab at the TU Darmstadt, researchers from Merck and the TU have simplified the diagnosis of bacterial infectious diseases. In doing so, they want to curb a global problem: the increase in multi-resistant germs that no longer respond to antibiotics.

By Uta Neubauer

"As much as necessary, as little as possible" should be the watchword when using antibiotics. But that is often not the case. The consequence: the drugs, once hailed as a miracle weapon, are failing in the fight against more and more disease-causing bacteria. Multi-resistant germs have become a dreaded problem, especially in hospitals. They lead to wound infections, blood poisoning or other diseases that are difficult or impossible to treat.

"According to projections, by 2050 more people will be dying from infections caused by resistant germs than from cancer," says Dieter Spiehl, researcher at the Merck Lab at the TU Darmstadt. In addition to the excessive use of antibiotics in mass animal husbandry, he also criticises the prescribing practice in human medicine. In a patient with cystitis, for instance, the type of bacteria causing the infection is not usually investigated. Most of the time coliforms are behind it, but sometimes staphylococcus or other bacterial pathogens are involved. This could be tested – classically with a culture in a Petri dish – and a specific remedy then prescribed. But only hospitals perform this as standard. "For practising doctors, the examination is too laborious and expensive. Instead, they prefer to prescribe broad-spectrum antibiotics," laments Spiehl. These preparations may fight the most diverse pathogens, but they also attack the body's own harmless bacteria. This not only leads to unwanted side effects, but also promotes the increase in resistant germs. Because whenever antibiotics are used, bacteria develop survival strategies. The most resilient survive and continue to spread.

"The tests are really simple and carried out without high-tech laboratory equipment"

The Merck Lab researchers now want to contain the problem with simplified diagnostic tools. "We want to replace the classic Petri dish with test cards," explains Gerhard Schwall of the Darmstadt-based science and technology company Merck, who heads the Merck Lab at the TU. Petri dishes are relatively large and, when filled with culture media, have only a limited shelf life. The cultivation of a culture also requires specialists trained in microbiology. Alternative analytical tools are already established in food production, where bacterial detection is a routine matter: test cards with printed culture media. They can be stored dry, require no refrigeration, and save space. Spiehl and his colleagues have applied this concept to medical diagnostics.

The test cards developed at the Merck Lab not only identify bacteria, but also detect antibiotic resistance. Their use is very simple. A member of staff at the laboratory or in the practice drips the patient's sample, for example a little urine, onto the card, covers it with a protective film and places it in a incubator overnight. The bacterial pathogens multiply and form bacterial colonies – as in the standard test in a Petri dish – that can be seen by the naked eye. The test field contains various detection reagents so that, for example, coliform bacteria appear as red dots, while staphylococcal colonies turn green. For the purpose of testing resistance, the test cards also contain various antibiotics. If the bacteria multiply in an area prepared like this, also identifiable by discolouration of the field, it means: attention – this antibiotic will not fight this pathogen!

Various printing methods are used in the production of the test cards. A screen printing machine using a viscous ink containing the nutrient medium and dyes for bacterial detection applies the test field onto a film. The liquid sample is later dripped onto this area. To prevent it from seeping beyond the field, a 3D printer prints a plastic outline around the test field. For resistance testing, droplets of various

Contact

Merck Lab @ TU Darmstadt
Project manager
Dr. Gerhard Schwall
Phone: +49(0)6151 16 23730
E-mail: gerhard.schwall@merckgroup.com
Dr.-Ing. Dieter Spiehl
Phone: +49(0)6151 16 22901
E-mail: spiehl@idd.tu-darmstadt.de
https://bit.ly/32pD7fG

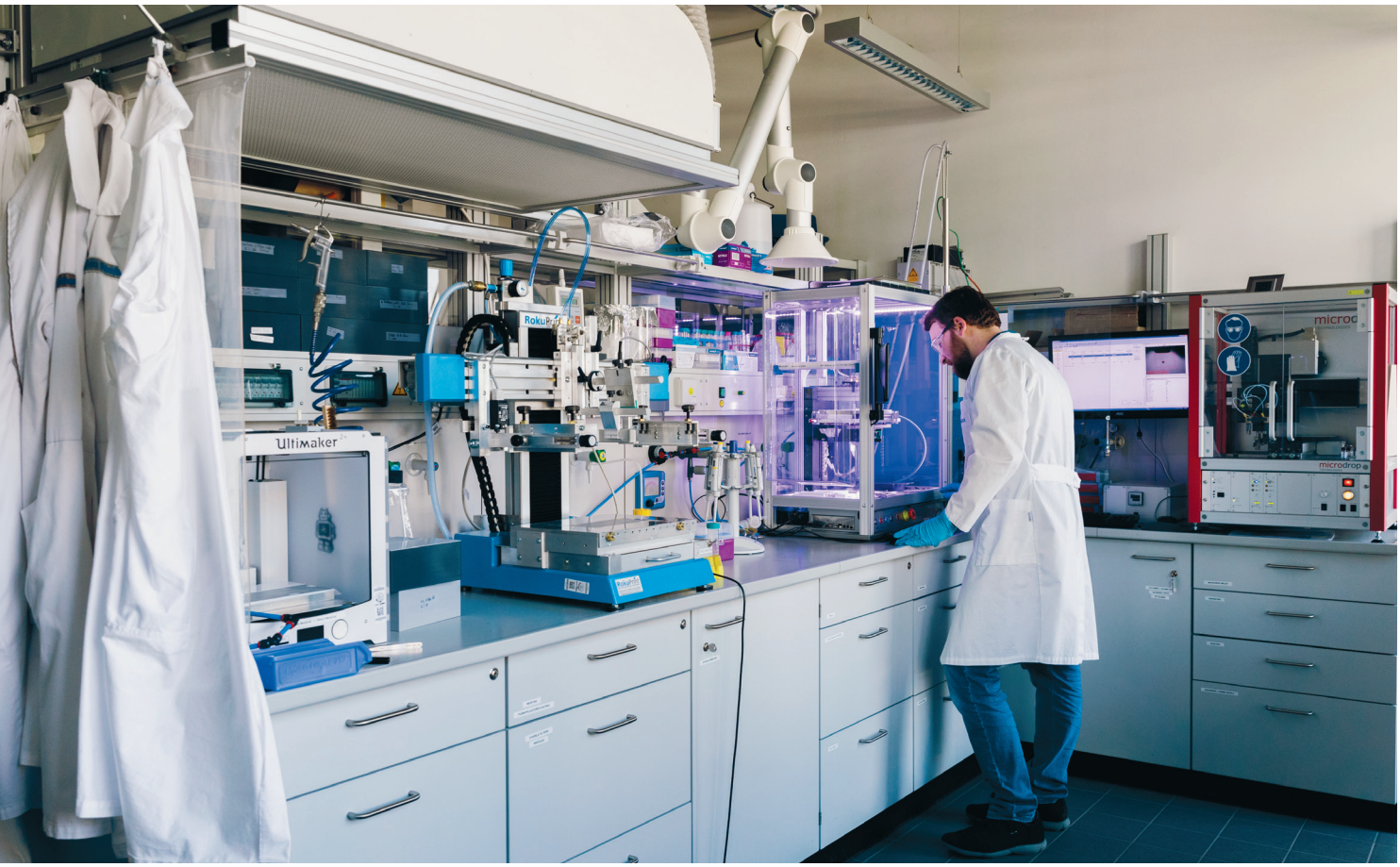
antibiotics are printed by ink jet onto certain spots inside the test field. Special printing strategies ensure that the antibiotics do not seep or even mix arbitrarily on the test field when the liquid sample is applied. Short legends and comparison fields for evaluation can also be printed directly onto the card. Finally, the system is given a transparent protective film that is folded up when the sample is applied. "We have already printed and used about 1500 test cards," estimates Spiehl.

With a doctorate in mechanical engineering Spiehl was already very familiar with printing techniques. His doctoral thesis focused on printing electronics, the focus of the Merck Lab at the time. Parallel to the current project, he is also leading a research group at the Institute of Printing Science and Technology (IDD) at the TU. He quickly became familiar with the topic of infectious diseases and their diagnosis in the multidisciplinary team of biologists and physicians. For three years, he and his colleagues tinkered with the design and production of the test cards. The result is impressive: "We have produced prototypes for various applications and demonstrated the feasibility of the concept," says Spiehl.

"The tests are so simple and can be carried out without high-tech laboratory equipment, which makes them ideal for small, less automated laboratories, even in developing countries," emphasises the head of the laboratory, Gerhard Schwall. The problem is serious in the world's poorest regions. Bacterial infections affect many more people there, while at the same time antibiotics are often used indiscriminately, thereby promoting resistance. "We discussed their needs regarding simplified diagnostics with doctors and laboratory technicians from European and African countries," says Spiehl. There is much interest from countries such as Nigeria and Zimbabwe: "We had already planned trials with two laboratory chains in Africa, but then the Corona pandemic came and we had to postpone the project indefinitely."

The new diagnostic tools have already been tested at Frankfurt University Hospital. Hundreds of samples, including from patients with urinary tract infections, were examined there with the test cards from the Merck Lab, always in parallel to the standard procedure in a Petri dish. "Step by step, we optimised our system and ultimately showed that it works," reports Spiehl with pleasure. Together with Merck, he and his colleagues are currently investigating commercial use. For the TU researchers, the project ends this year. It is to be hoped that the test cards will be developed quickly to market maturity and thus make a valuable contribution in the fight against antibiotic-resistant germs.

The author is a science journalist with a doctorate in chemistry.



Various printing methods are used to produce test cards at the Merck Lab at the TU that will facilitate simplified diagnosis of infectious diseases in the future.

Photo: Katrin Binner

Race against the big code breaker

Photo: Ralf Werner

Post-Quantum cryptography is the research topic of Juliane Krämer, mathematician and computer scientist at TU Darmstadt.

Quantum computers may be able to crack the encryptions common in the network in ten years – even retroactively. The Darmstadt cryptographer Dr. Juliane Krämer counters with mathematics.

Von Christian J. Meier

"Imagine yourself in the near future, and picture a website where anyone could see your WhatsApp communication of today," says Dr. Juliane Krämer. "At what point wouldn't that bother you any more? In a year? In ten years?" asks the researcher from the profile area CYSEC of the TU Darmstadt. Krämer combines the question with a warning: in just a few years' time, there could be a quantum computer that cracks the encryptions that are common in the Internet today. At the collaborative research centre CROSSING, the cryptographer is developing new methods that will defy code-breakers – a field that is known as post-quantum cryptography. She believes that, depending on the need for protection, we should already be arming ourselves against the computers of tomorrow.

Contact

Research Group Quantum and Physical attack resistant Cryptography (QPC)
Dr. Juliane Krämer
Phone: +49(0)6151/16–20662
E-mail: juliane@qpc.tu-darmstadt.de
www.informatik.tu-darmstadt.de/qpc

The threatened measures protect against eavesdroppers and generate digital signatures without which online banking or software updates would not be trustworthy. To encrypt data, the sender turns them into "mojibake", a jumble of characters that only the recipient can untangle. In order to prevent the two from having to exchange a secret key, so-called "asymmetric cryptography" are used. The recipient, perhaps a bank, makes the key available to the public. This allows the sender to easily encrypt their message to the bank. However, the public key cannot be used for decryption. For this purpose, the recipient alone has a "private key". This is achieved with a kind of mathematical hub, which can be passed in one direction without resistance (encryption by public key). However, when moved in the other direction, it is blocked. Only the owner has a key that unlocks the locking mechanism (decrypting it with the private key) and lets it pass in the blocked direction. Digital signing works in the same way, only with the inverse flow of information: the sender uses their private key to create the electronic signature. The recipient can check their authenticity with the public key.

Today's most widely used "hub" works with very large prime numbers. Multiplying two prime numbers is easy. The reverse way of breaking down the product into its prime factors, however, is so difficult that even a supercomputer would take decades to do so. Anyone can use the product as a public key for encryption. Only the recipient knows the prime factors that they can use as the private key. Every day, this so-called RSA method and related methods secure communication billions of times on the Internet. However, this could be over in one fell swoop once a high-performance quantum computer is ready. Because the digital hubs currently used are precisely not that for it. It will perform the reverse calculation at lightning speed.

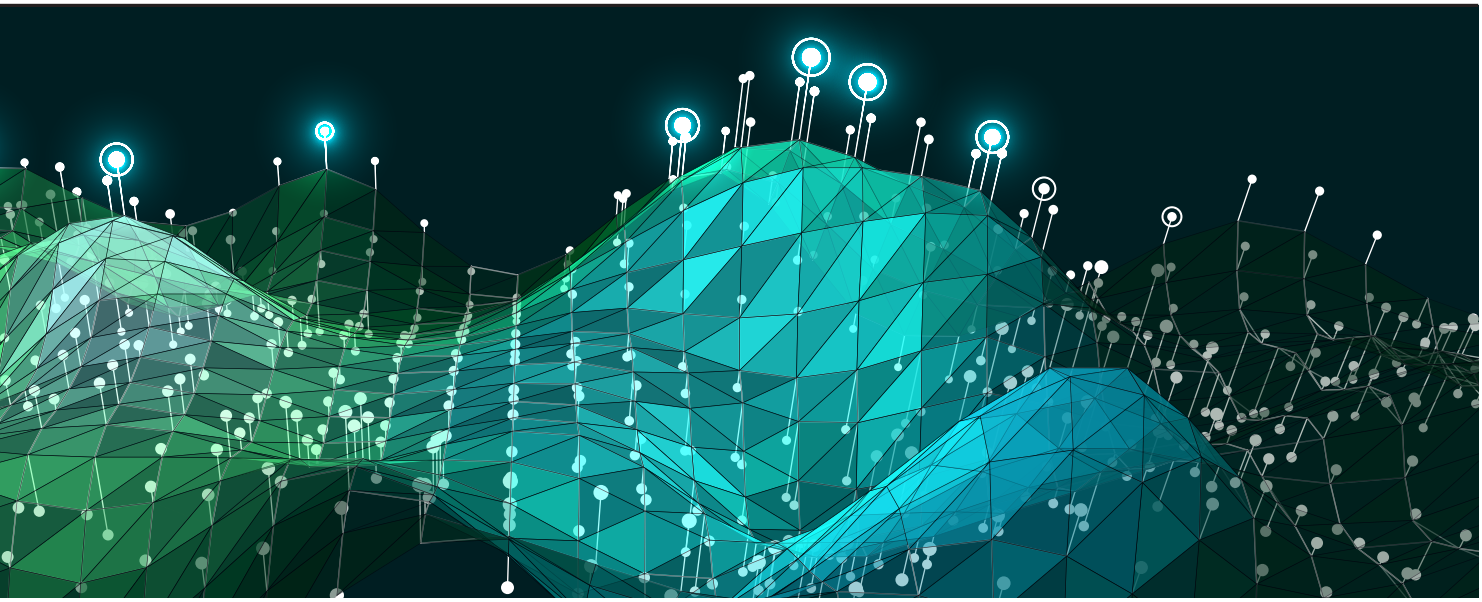


Photo: Adobestock

Juliane Krämer is researching new post-quantum methods to protect against quantum computers of the future.

However, the quantum computer will not be an all-rounder. Only a few problems are known, and their resolution will accelerate radically. Researchers believe that it will not be able to solve many problems faster, if at all, than a normal computer. These include other mathematical hubs from the ones currently used in cryptography. Specialists such as Juliane Krämer develop new crypto methods from this. "Post-quantum cryptography is a very active field of research," says the mathematician and computer scientist. She herself is researching so-called "lattice-based cryptography". By "lattice", mathematicians mean a space filled with a regular arrangement of "lattice points". A construction fence resembles a lattice with two dimensions: the intersections of the wires form the lattice points. It is easy for mathematicians to span lattice with hundreds of dimensions – obviously only as a virtual entity. Now an additional point can be added anywhere between the individual lattice points. Because of the many dimensions, it can be extremely difficult to find the next lattice point. But it can also be easy. It depends on how the lattice is described mathematically. Mathematics speaks of a "good" or a "bad" basis. If a "bad basis" is used as the public key and a "good" one as the private one, then a mathematical "hub" has been created.

"Post-quantum cryptography is a very active field of research."

This and similar problems have been known for a long time. "However, which problems will prevail as highly relevant in practice and which will not has yet to be revealed," says Krämer. Development teams were still looking for a suitable balance between security and efficiency of the procedures. The researchers are playing with, for instance, different mathematical representations of lattices. Computational operations run faster with one of them, in the form of "polynomials". But the keys require a relatively large amount of storage space, which is a disadvantage for mobile applications such as mobile phones. "There is no one-size-fits-all solution for increasing efficiency," says Krämer. Creativity is required.

Research teams create many methods with various advantages and disadvantages in terms of securety and efficiency. In 2016, the American standardisation authority NIST called for a process, and around 80 proposals were received in response. After an initial evaluation, 29 methods remained. Most of them are lattice-based. NIST identified weaknesses in the individual procedures, and called on the authors to make improvements. "The methods are public," explains Krämer. Industry colleagues find security gaps that the originators then plug. In the meantime, NIST has further restricted the field of applicants. Juliane Krämer is also working on test methods to ensure that new post-quantum methods actually do protect against quantum computers. However, there can never be absolute certainty, as uncrackability is always based on assumptions even with the procedures currently in use.

Until the standards for post-quantum cryptography have been established, there will always be a kind of encryption gap, warns Krämer. While digital signatures only need to be safe for the moment, encrypted data should often remain so permanently. In a few years' time, today's ciphered data could be cracked by a quantum computer. Anyone who wants to remain on the safe side in the long term should stop using RSA and the like today, advises the cryptographer. Numerous methods are entirely ready for use.

The author is a science journalist with a doctorate in physics.

Links and publications:

Collaborative research centre Crossing at the TU Darmstadt:
www.crossing.tu-darmstadt.de/crc_1119/index.en.jsp

Profile area Cybersecurity (CYSEC) at the TU Darmstadt:
www.cysec.tu-darmstadt.de/cysec/index.de.jsp

Podcast:
https://www.hessen-schafft-wissen.de/podcast/Juliane-Kraemer

Current publication: Krämer, Struck (2020): Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security. PQCrypto, 2020, Paris, France

Quick facts

Scientists at TU Darmstadt shed some light on the theme of passenger information in trains operated by DB Regio AG.

By Astrid Ludwig

Discovering that the train you have booked is on time but full or is late or cancelled due to a disruption is a fairly common experience. What information would commuters and leisure travellers like to receive during normal service and in the event of a disruption? When and how should this information be made available on regional and local trains and what information channels should be used? Researchers at TU Darmstadt and DB Regio AG are investigating how modern, needs-based and flexible passenger information should be organised as part of an innovation alliance formed by the university and Deutsche Bahn.

"The methods used to provide information are not keeping pace with the latest developments in digitalisation and IT", says Manfred Boltze, Professor and Head of the Institute of Transport Planning and Traffic Engineering at TU Darmstadt. Trains are often old and the technology is not fully up-to-date. He believes that existing methods used to provide passenger information visually and acoustically increasingly appear outdated, static and – due to the long contractual terms for the installed systems – lacking in innovation. In order to develop a new concept that specifically focuses on the needs of train passengers, the researchers have surveyed around one thousand train customers. The questionnaire was developed in cooperation with experts from Deutsche Bahn for daily commuters and other travellers who use local trains in the Rhine-Main region. In particular, the questionnaire was designed with the aim of finding out when passengers would like to receive which information, how loud the announcements should be, where instructions should be displayed so that they can be easily seen and what questions and answers are a priority, for example, in the event of a disruption to the service. The most important finding from the survey is that there is hardly any difference in the need for information amongst commuters, leisure travellers, students and old or young people. "This surprised us. We expected to find greater differences between the groups", says Professor Boltze. According to the findings, all of the groups would mainly like to receive information on punctuality, arrival and departure times and alternative connections in the event of a delay or disruption to the service. "They want to receive hard facts in a prompt, reliable and easy to understand manner", summarises Manfred Boltze.

Contact

Institute of Transport Planning and Traffic Engineering
Prof. Dr.-Ing. Manfred Boltze
Phone: +49(0)6151/16 – 22500
E-Mail:
boltze@verkehr.tu-darmstadt.de
www.tu-darmstadt.de/verkehr
DB Regio AG
Dr.-Ing. Leif Fornauf
E-Mail:
Leif.Fornauf@deutschebahn.com

Almost half of those surveyed would like information on how full the train currently is and already want to receive this information at the station while they are waiting for the train to arrive. Around 60 percent of those surveyed would like more information to be displayed or announced in the event of an interruption to the journey. In general, passengers want information on the train service itself; information on the weather, news or advertisements are of secondary importance or uninteresting for most passengers. According to Boltze, it is important to provide consistent information in a timely manner so that the same information is available across all information channels and there is no confusion. More than 80 percent of passengers own a smartphone with an installed travel app and over 60 percent of them use this app often or even on every single journey. Nevertheless, more than 30 percent of the passengers stated that they mainly use train media to access information during the journey.

It is thus vital that this information is up-to-date, modern and easy to see or hear – even for persons with reduced mobility. The researchers at TU Darmstadt believe that there are good opportunities for providing quick and comprehensive information using, amongst other things, directional speakers, side panel displays, information points and additional displays installed in the train compartments which indicate whether there are free seats or luggage compartments.

The author is a scientific journalist.

Further Information

The short report "Modern passenger information – providing needs-based, flexible and innovative information to passengers travelling on regional trains" will be published shortly at **https://www.verkehr.tu-darmstadt.de/vv/das_institut_ivv/**

Further information on the innovation alliance between TU Darmstadt and Deutsche Bahn: **https://bit.ly/2XXHlK4**

Photo: Deutsche Bahn AG / Volker Emersleben

The Institute of Transport Planning and Traffic Engineering is investigating which information is particularly important for train passengers.