
CROSSING
Cryptography-Based Security Solutions
Enabling Trust in New and Next Generation Computing Environments
NEXT LEVEL SECURITY

*» Cryptography needs to evolve constantly in order to address today's and tomorrow's challenges.*

Marc Fischlin is Professor of Cryptography and Complexity Theory at the Technische Universität Darmstadt.

Photo: Katrin Binner

Photo Cover: Jan-Christoph Hartung
Design: SCHUMACHER — Brand + Interaction Design

*Mission Statement*

***CROSSING provides cryptography-based security solutions enabling trust in new and next generation computing environments. The solutions meet the efficiency and security requirements of the new environments and have sound implementations. They are easy to use for developers, administrators, and end users of IT, even if they are not cryptography experts.***

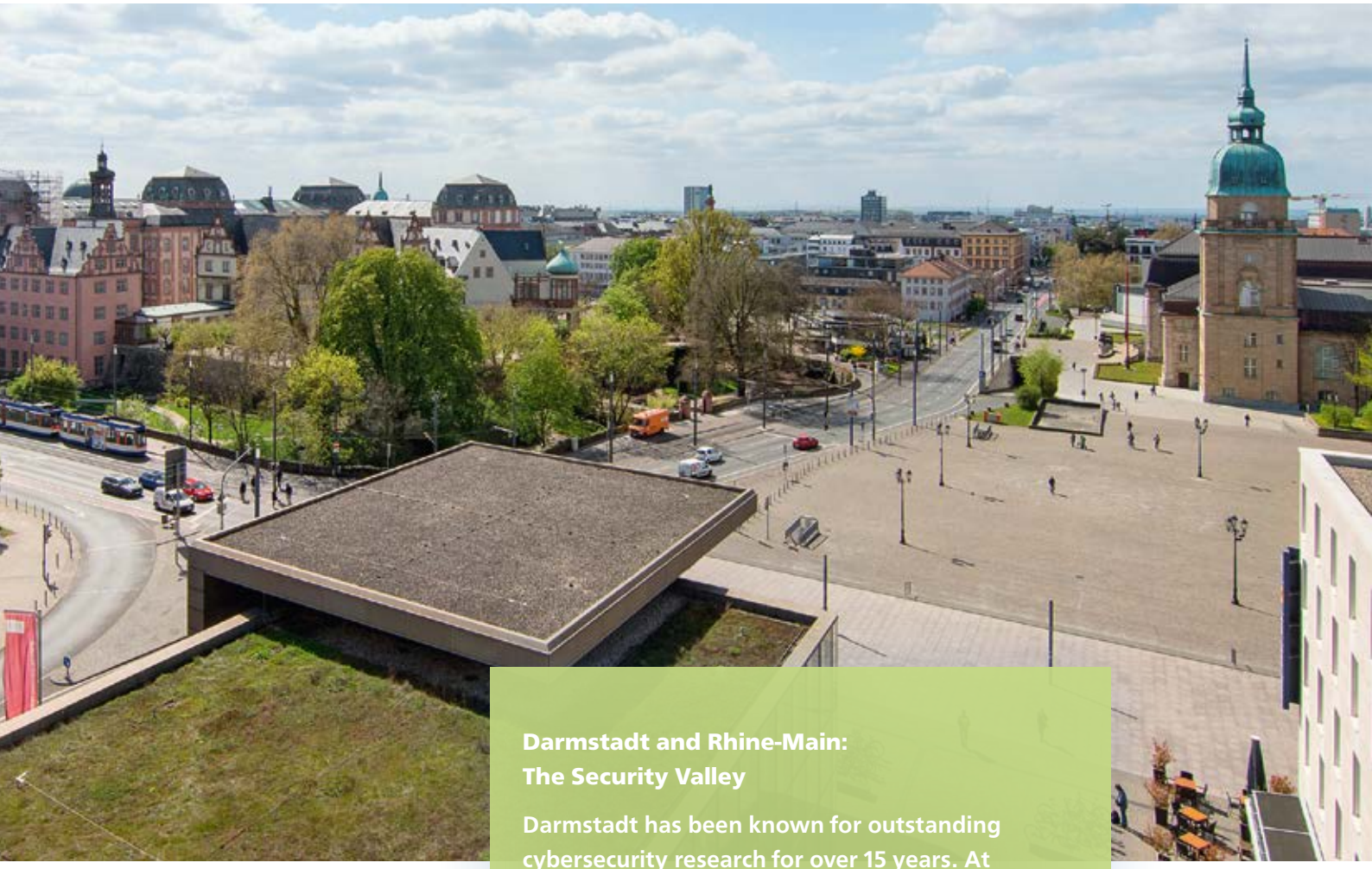


Photo: Patrick Bal / TU Darmstadt

## Darmstadt and Rhine-Main: The Security Valley

Darmstadt has been known for outstanding cybersecurity research for over 15 years. At Technische Universität Darmstadt cybersecurity is an integral part of the research profile of the university. CROSSING was the first Collaborative Research Center funded by the German Research Foundation (DFG) in the field of cryptography, and its funding is a great success for Darmstadt and the university. To further strengthen the excellent research in this field, cybersecurity was announced as one of six profile areas of TU Darmstadt. The university is also a member of the National Research Center for Applied Cybersecurity, which is one of the largest cyber-security research centers in Europe.

*Interview*

# FACING THE CHALLENGES OF THE QUANTUM ERA

**Interview with Johannes Buchmann**

Johannes Buchmann is Professor of Cryptography and Computer Algebra at the Technische Universität Darmstadt.

**Professor Buchmann, if a group of criminal hackers were to secretly develop a quantum computer, what would happen if they used it in an attack?**

JB: Quantum computers can find secret keys and forge security certificates. The criminals might start by forging the signatures of software programs and penetrating the operating systems, software and apps of all computers and smartphones that rely on similar protection mechanisms and are connected to the Internet. After that, they could either shut down the devices and demand a ransom, or they could secretly monitor and control them. As a next step, the criminals could crack all cryptographically secured Internet communications – such as during online banking, or encrypted emails. A hacker could also pretend to be someone else. And finally, the owner of a quantum computer could decipher and read information encrypted in the past. That could do a lot of harm.

**IBM presented a quantum processor with 50 quantum bits [qubits], Google one with 72 qubits. The Canadian D-Wave Systems has even presented a complex system of more than 2,000 qubits. When do these start to become a threat?**

JB: The computers would need millions of qubits. However, that is not to say this may not be possible in the foreseeable future. The Canadian mathematician and quantum scientist Michele Mosca has extrapolated available data and predicted that the risk of quantum computers compromising key methods by the year 2026 is one in seven. By 2031 the risk will have risen to 50%. Many scientists consider his study to be plausible.

**How close are cryptographers to developing methods that cannot be cracked by such computers?**

JB: The first international conference on post-quantum cryptography was held in 2006. Since then, research institutes all over the world have been working on the problem. Here in Darmstadt we developed the first post-quantum signature scheme ever standardized. At the moment, the US National Institute of Standards and Technology (NIST) is working on a standardization procedure for quantum-secure cryptography. Researchers have submitted 70 procedures they consider to be quantum-secure. We at CROSSING have also submitted a proposal that has already made it to the second round of the competition. So, there are a number of promising candidates that could solve the problem.

But there are two obstacles that need to be overcome – by cryptographers, standardizers and IT manufacturers. The first is time: can we develop the methods and incorporate them into the programs more quickly than the developers of quantum computers make advances with their machines? Our past experience has been that it takes longer than one would like, but I remain


*» Sustainable cybersecurity is possible.*

Photo: Gregor Rynkowski

optimistic, especially since the developers of quantum computers face greater technical challenges than we do.

The second obstacle is more fundamental. When you develop a cryptographic method, you can never be 100% certain that it really is secure. Some clever brain somewhere in the world could come up with a mathematical or technical loophole we have overlooked. That has already happened in the past, but was not as serious then as it would be today, because the world did not rely on computers to the extent that it does now.

**Does a form of cryptography exist that will be safe for all time?**

JB: It is mathematically possible. And you can also use quantum communication technologies to exchange keys in ways that are 100% secure. We are in the middle of researching this, to provide long-term protection for hospital data in Japan, but it is moving slowly and at the moment is only a niche market.

**Source: This interview was shortened and slightly updated from the article "A quantum of menace" by Thomas Ramge, published in the magazine brand eins 03/2018, https://international.brandeins.de/a-quantum-of-menace.**

### Quantum computers

**A classical computer uses bits to represent data, where a bit can be in one of two states: 0 or 1. A quantum computer uses qubits to represent data. Quantum mechanics allows qubits to be in states 0 and 1 simultaneously, rather than being exclusively in either of these states. This effect is known as 'superposition' and allows to speed up computations. Another important effect is 'entanglement', which creates some form of dependence between different qubits. Due to these two quantum mechanical effects, a quantum computer can solve problems which cannot be solved on a classical computer. Beside the positive effects induced by quantum computers, for instance when developing new vaccines, they also pose security risks as they are able to break the cryptography that is currently used to secure communication on the Internet. Another risk is that an attacker can record encrypted data today and could, in several years when quantum computers exist, break the encryption. Thus, alternative cryptography, which is secure against quantum computers, must be developed today.**

## Sustainable security

**Health records must be stored securely for a lifetime or even multiple generations. CROSSING researchers developed a solution that will ensure everlasting safe storage for sensitive health data in a joint project with Japanese and Canadian partners. The "LINCOS – Long-Term Integrity and Confidentiality Protection" system is the first to combine information-theoretic confidentiality protection with renewable integrity protection. An initial prototype has already gone into successful trial operation in Japan.**

Photo: Jan-Christoph Hartung

*Research*

# GREAT IMPACT AND INTERNATIONAL VISIBILITY

In the future, digital attacks will become more and more powerful, especially with enormously potent quantum computers. Cryptography is an essential enabler of trust in IT systems. However, current cryptography is inadequate, due to the lack of functionalities, sound implementations, resistance against future attacks, and usability.

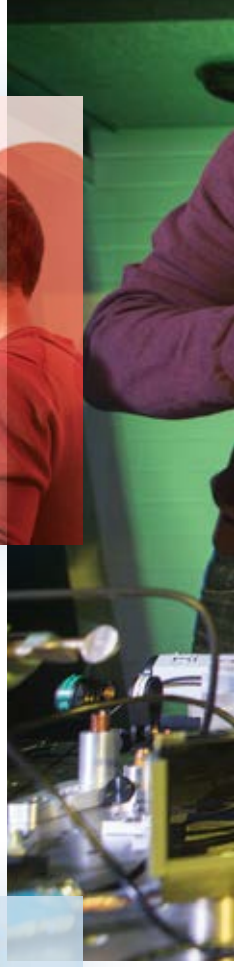
CROSSING research focuses on cryptography-based security solutions for long-term trustworthy computing environments. With excellent, internationally visible results our CROSSING scientists contribute significantly to making the digital world safer and protecting our privacy. To achieve this, CROSSING brings together an interdisciplinary team of highly qualified researchers. Specialists in cryptography, system security, and network security design cryptography-based security solutions. Hardware- and software-oriented cryptographers including experts from high-performance computing, complexity theory, and quantum physics provide secure cryptographic primitives as building blocks for the solutions. Researchers from the areas of software technology, formal methods, and security engineering provide secure implementations of security solutions as well as means to allow easy integration into complex applications. This is a unique collaborative effort of research areas that were far too isolated from each other before CROSSING was founded.

The CROSSING research program is dynamically adjusted for the technological developments and expectations, to ultimately provide a coherent framework of methodologies and technologies that allows rapid and flexible means of addressing the highly complex IT security challenges of the future. For example, the protection of trillions of networked devices in the Internet of Things (IoT) and the security of block-chain applications like cryptocurrencies or Smart Contracts have been incorporated into the research program.

Our results and achievements have had significant impact on the international development of IT security research and will continue to do so. This innovative, collaborative effort has made significant progress towards safety in the digital world. Highlights of the first phase included the development of new quantum attack-resistant encryption and signature schemes that are currently being evaluated as international standards, as well as the intelligent crypto-assistant CogniCrypt which has recently become part of Eclipse, one of the most frequently used software development platforms worldwide. Our results have been presented in over 300 publications, more than one third of which have been published at top tier security and privacy conferences. More than half of these publications resulted from national and international collaborations within the scientific community as well as our partners from industry, such as Oracle, Cisco, Intel or Deutsche Telekom.

*People*

# CROSSING THE BOUNDARIES OF DISCIPLINES



CROSSING is a unique collaborative effort: highly qualified researchers from quantum physics, cryptography, system security and software engineering design, build and implement cryptography-based security solutions. To solve the security issues of new and next generation computing environments it is necessary to move in new directions. Research areas that worked in isolation from each other before CROSSING began, now work together to contribute to the joint goal. The success of CROSSING lies in the extraordinary dedication and team spirit of individual researchers combining their strengths. CROSSING actively encourages collaboration and team building in various ways. Twice annually a retreat with all CROSSING members takes place in a relaxed atmosphere where collaborations can be commenced and further developed. To encourage collaboration, the CRC established the CROSSING Collaboration Award which is presented for excellent internal collaborative work and outstanding progress in research collaborations within CROSSING. It is awarded annually and rewarded with a trophy and funds for conference or workshop participation

CROSSING offers an Integrated Research Training Group (IRTG) for its junior researchers to support them in pursuing their doctorate and their academic career. As well as offering close supervision, this includes qualification courses tailored to the needs of security researchers.

Gender-equality and family-friendly measures are implemented to ensure that all participants have the same opportunities in CROSSING. Child-friendly work spaces and a mobile childcare unit called “KidsBox” are two resources for parents in CROSSING. To encourage female students to consider a career in computer science, there is also a mentoring program which includes opportunities for student and mentor to attend conferences together.

Photos: Jan-Christoph Hartung; Group photo: Ann-Kathrin Braun

*Structure*

# A UNIQUE INTERDISCIPLINARY COLLABORATION

CROSSING is a Collaborative Research Center funded by the German Research Foundation. It is a long-term university-based research institution with a 12 year lifespan, in which researchers work together within a multidisciplinary research program. To overcome the roadblocks to our overall goal – cryptography-based security solutions enabling trust in new and next generation computing environments – CROSSING is divided into three research areas: Solutions, Primitives, and Engineering. These correspond to the three major challenges to the CROSSING goal. Each area contains projects which envision and devise solutions for these challenges.

All three project areas collaboratively develop CogniCrypt, our intelligent open-source assistant for software developers ensuring the secure usage of crypto components. CogniCrypt supports users in specifying their requirements for cryptography-based security solutions, provides sound implementations of such solutions, helps users to correctly integrate them into their projects, and to update them if required. The solutions developed in the project areas are integrated into CogniCrypt and made available to other researchers and software developers.

Collaboration within CROSSING and with international partners is vital to success. For example, the design of the solutions determines requirements for primitives, and developing techniques that enable secure and easy integration of security solutions into applications becomes possible through close collaboration with the solutions designers. In particular, the development of CogniCrypt driven by the Engineering project area requires strong interaction between all CROSSING members.

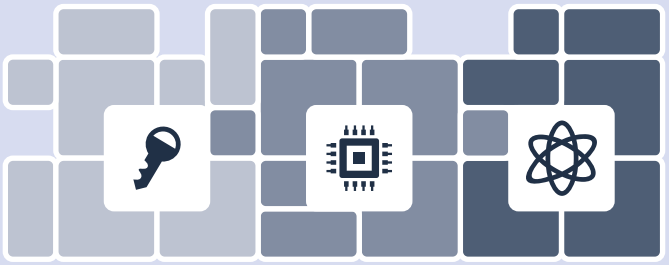
Collaboration and participatory structures are also important in the organizational structure of CROSSING: The directorate, responsible for strategic decisions regarding CROSSING, incorporates members from all status groups. In addition to constant internal evaluation, external experts in an advisory board with renowned researchers give feedback on CROSSING's scientific achievements on a regular basis.

**Facts & Figures**

- **Collaborative Research Center (CRC), funded by the German Research Foundation (DFG)**
- **CROSSING was established at TU Darmstadt in 2014 and cooperates with the universities of Paderborn and Duisburg-Essen**
- **Planned completion year 2026**
- **Total research budget for the second funding phase (2018 – 2022): ~11 million Euros**
- **65 researchers from 17 research groups (15 at TU Darmstadt, one each at the universities of Paderborn and Duisburg-Essen)**
- **22 full research positions funded through CROSSING**

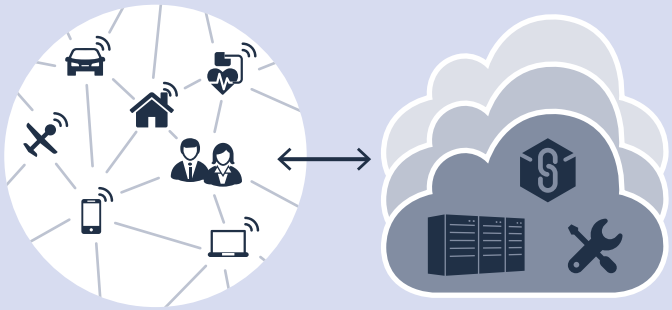
# PRIMITIVES

Cryptography-based security solutions rely heavily on cryptographic primitives such as encryption and signature schemes. However, existing primitives are threatened by attacks which are made possible by new computing architectures and algorithms. New cryptographic solutions require efficient primitives with new functionalities such as sanitizable signatures. Thus, a major challenge is the development of the required cryptographic primitives. They must be efficient in present and future computing environments, and they must resist attacks due to new hardware platforms and algorithmic advances. The goal of this area is to develop primitives that are required to build cryptography-based security solutions, in particular those of the Project Area Solutions, and to provide sound realizations in collaboration with Project Area Engineering.



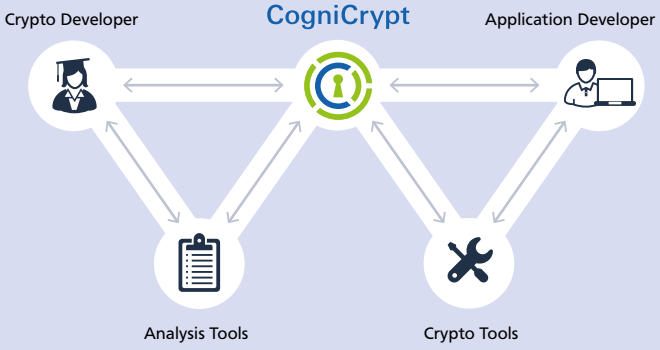
# SOLUTIONS

The goal of this area is to provide cryptography-based security solutions that match all the necessary functional requirements to establish trust in new and next generation computing environments. This includes the development of new trust-establishment methods both in individuals and devices, novel ways to secure critical communication, and new techniques to improve the security of remote services. Such solutions will be indispensable when establishing trust in the identities and properties of actors, the soundness of their devices, and in the proper functioning and privacy-friendliness of services. This is even more true in distributed and highly connected environments.



# ENGINEERING

Cryptography-based security solutions and cryptographic primitives can engender trust only if their implementations can be trusted, i.e., if secure implementations exist, and if users and developers are supported in integrating them correctly into their applications. The goal of the Project Area Engineering is to develop technologies that allow for secure implementations of cryptography, enable developers to securely integrate primitives and solutions even if they are not cryptography experts, and provide tools that support the automatic generation and usage of security and privacy solutions.



*Real-world applications*

# COGNICRYPT – A TRULY SMART CRYPTO ASSISTANT

**Supporting software developers by ensuring the secure usage of crypto components to protect users' data**

Software security often equals data security. Studies show that over 75% of applications embed cryptography in an insecure way which puts user data such as credit card information or sensitive personal data at risk. Why does this happen?

Despite the fact that security features, mostly involving cryptography, are required in almost every application, software developers usually have no experience with cryptography – and therefore implement the crypto components incorrectly.

That's why CROSSING scientists created CogniCrypt, an intelligent platform that helps developers to securely integrate encryption and other crypto components into their applications in an easy, user-friendly way. The goal of CogniCrypt is to significantly increase the security of software applications. CogniCrypt has been designed to seamlessly integrate into developers' workflows because it is part of the popular Eclipse platform already used by millions of software developers.

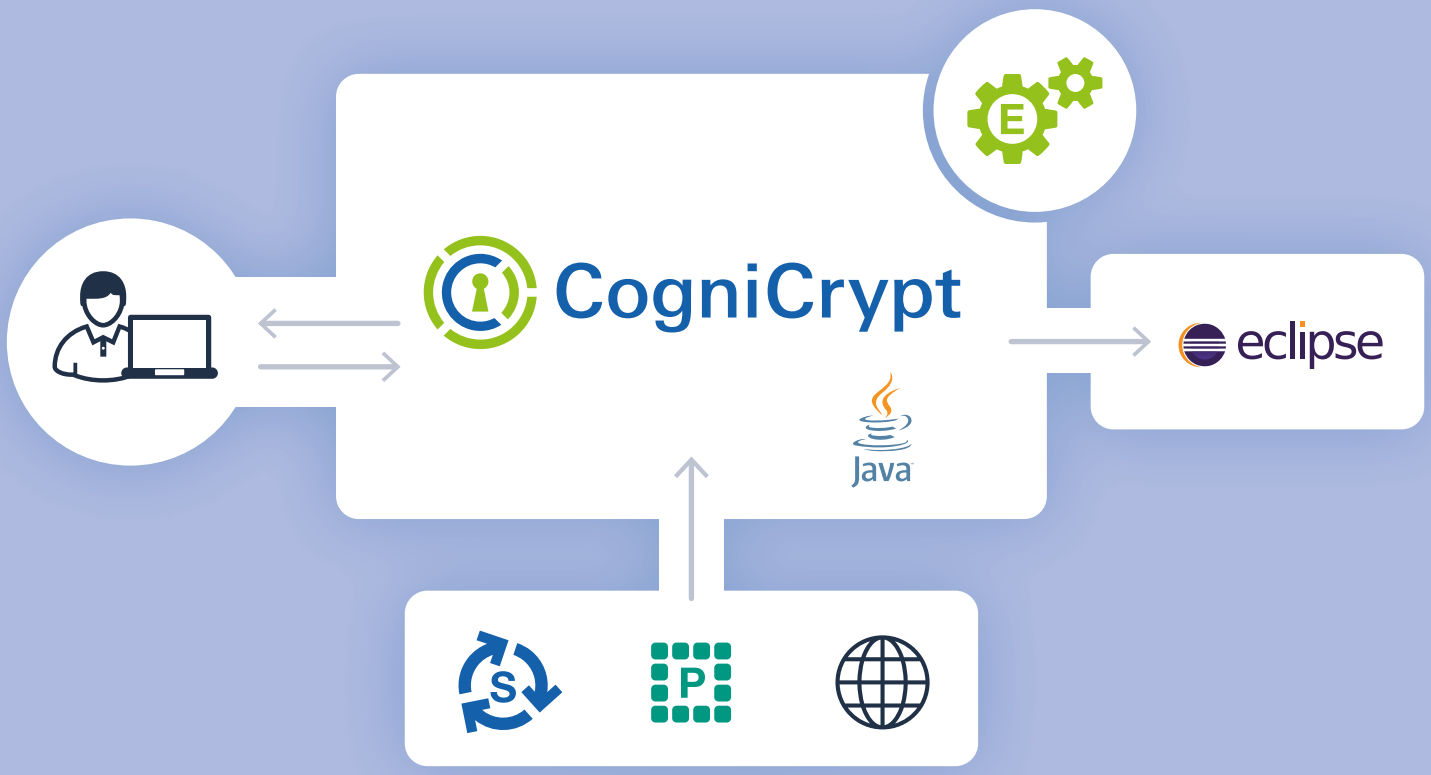
CogniCrypt allows developers to automatically generate code for the secure integration of cryptography. It actively assists application developers in selecting and correctly integrating its components into applications. Another feature is that it recognizes crypto misuse in (existing) program code and, if detected, provides advice on how to fix this vulnerability – in a text-based way without the need for expert knowledge.

CogniCrypt is open-source. This allows experts from other universities, research institutions and companies to verify whether the provided usage rules, advice and implementations are accurate. In addition, security experts, cryptographers and software developers can provide feedback or suggest and contribute new features and crypto components. Join us and become part of the vibrant community of CogniCrypt!

@cognicrypt

www.cognicrypt.org

CogniCrypt is a joint project of CROSSING at TU Darmstadt, University Paderborn and the Fraunhofer IEM Institute. The development of CogniCrypt is officially supported by Oracle and the German Federal Office for Information Security (BSI). It was awarded the status of an official Eclipse project in December 2017.



*Contact*

# ARE YOU INTERESTED?

Want details about our research topics?
Interested in collaborating with us? Starting your career in research?
Planning an article, broadcast or podcast on cybersecurity topics?
Please contact us and we will be happy to assist you.

**Johannes Braun**
Manager
T: +49 (0)6151 16-20664
E: jbraun@cdc.informatik.tu-darmstadt.de

**Ann-Kathrin Braun**
Public Relations
T: +49 (0)6151 16-22662
E: akbraun@cysec.tu-darmstadt.de

**Visit us online:**

**www.crossing.tu-darmstadt.de**

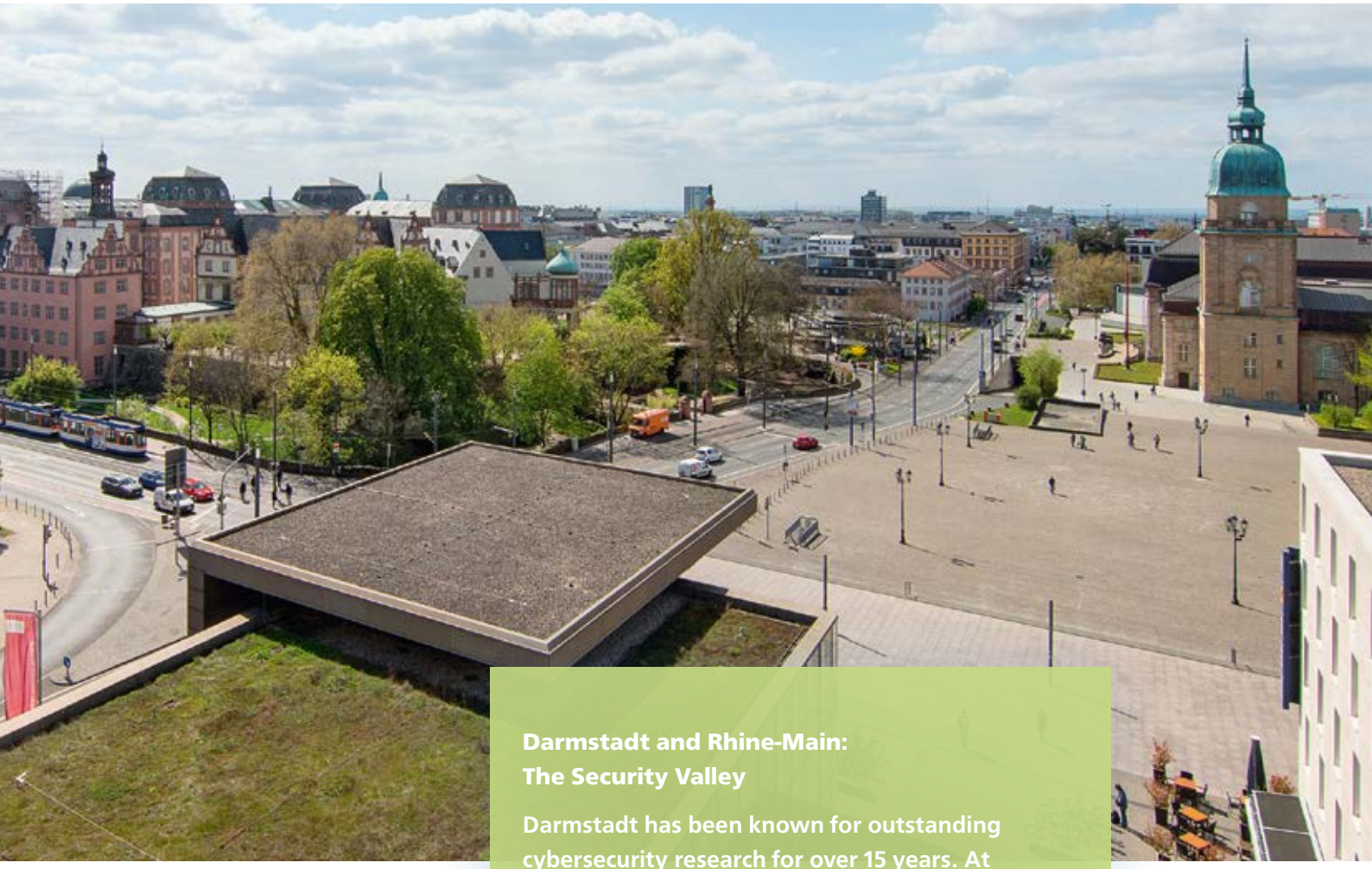
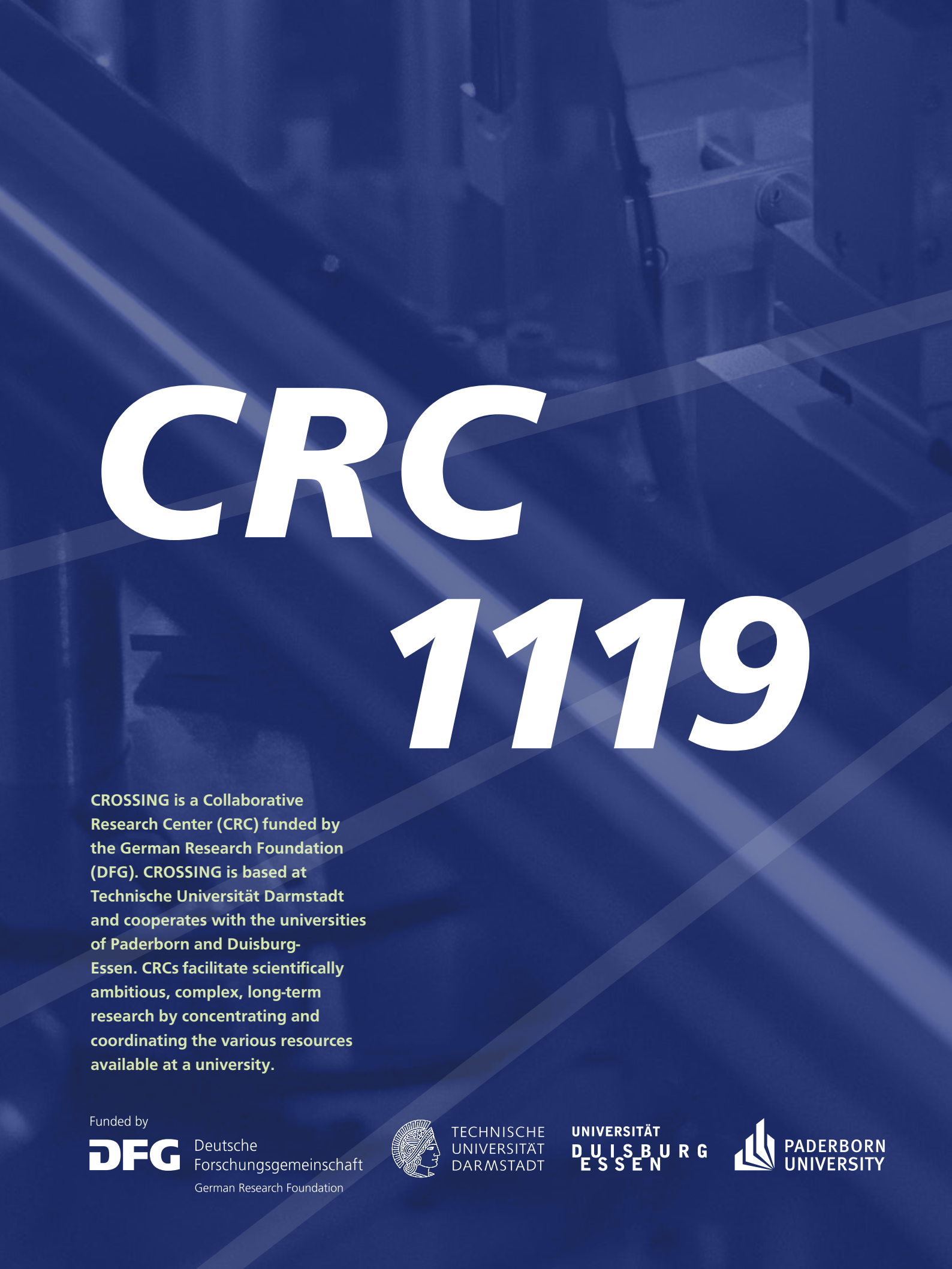


Photo: Patrick Bal / TU Darmstadt

## Darmstadt and Rhine-Main: The Security Valley

Darmstadt has been known for outstanding cybersecurity research for over 15 years. At Technische Universität Darmstadt cybersecurity is an integral part of the research profile of the university. CROSSING was the first Collaborative Research Center funded by the German Research Foundation (DFG) in the field of cryptography, and its funding is a great success for Darmstadt and the university. To further strengthen the excellent research in this field, cybersecurity was announced as one of six profile areas of TU Darmstadt. The university is also a member of the National Research Center for Applied Cybersecurity, which is one of the largest cyber-security research centers in Europe.



# CRC 1119

**CROSSING is a Collaborative Research Center (CRC) funded by the German Research Foundation (DFG). CROSSING is based at Technische Universität Darmstadt and cooperates with the universities of Paderborn and Duisburg-Essen. CRCs facilitate scientifically ambitious, complex, long-term research by concentrating and coordinating the various resources available at a university.**

Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

TECHNISCHE UNIVERSITÄT DARMSTADT

UNIVERSITÄT DUISBURG ESSEN

PADERBORN UNIVERSITY