Universität der Bundeswehr München

CODE
ANNUAL REPORT
2024

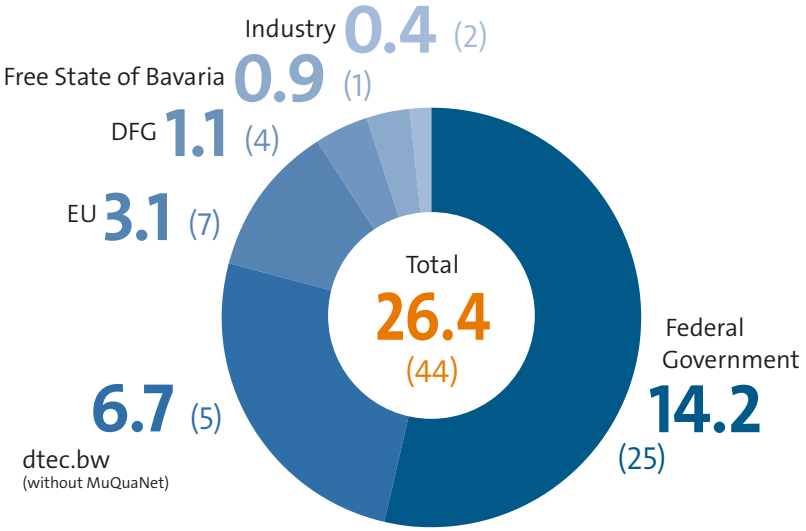
CODE RI

Research Institute
Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2024, a total of 44 projects financed by third-party funds were either processed or acquired. dtec.bw projects receive funding from the budget of the BMVg division.

Third-Party Funds*



* Numbers (rounded) in millions of euros, quantity of projects in parentheses.

dtec.bw Project**

MuQuaNet—The Munich Quantum Network

MuQuaNet
The Munich Quantum Network

Participating Professorships

Prof. Dr. Wolfgang Hommel
Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Arno Wacker

** With participation of RI CODE and project start in 2020; not included in the third-party funds overview (left).

Internationality

RI CODE maintains a large international network.

Employees***

In 2024, CODE employees came from 17 countries.

Cooperation Partners***

In 2024, RI CODE cooperated with 76 partners in 26 countries.

Legend

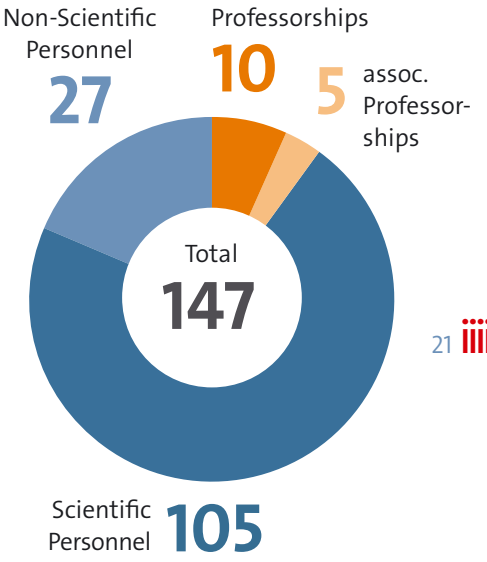
- Location of RI CODE
- 1 — Number of CODE employees from the country of origin
- 1 — Number of international cooperation partners in the respective country
- Countries with cooperation partners and employees

*** More information about contacts and cooperation partners can be found from p. 88 onwards.

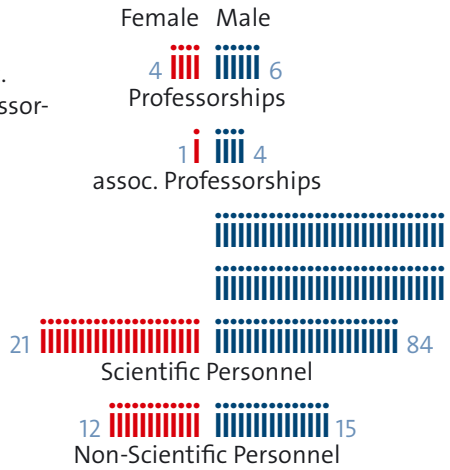
Staff Structure

**RI CODE had a total of 147 employees in 2024.
26% percent of the staff were women.**

Employees



Gender Share



26% **74%**

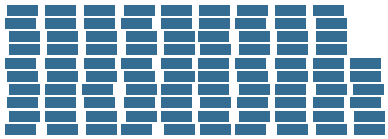
Research Work

Overview of doctorates and publications at RI CODE 2024

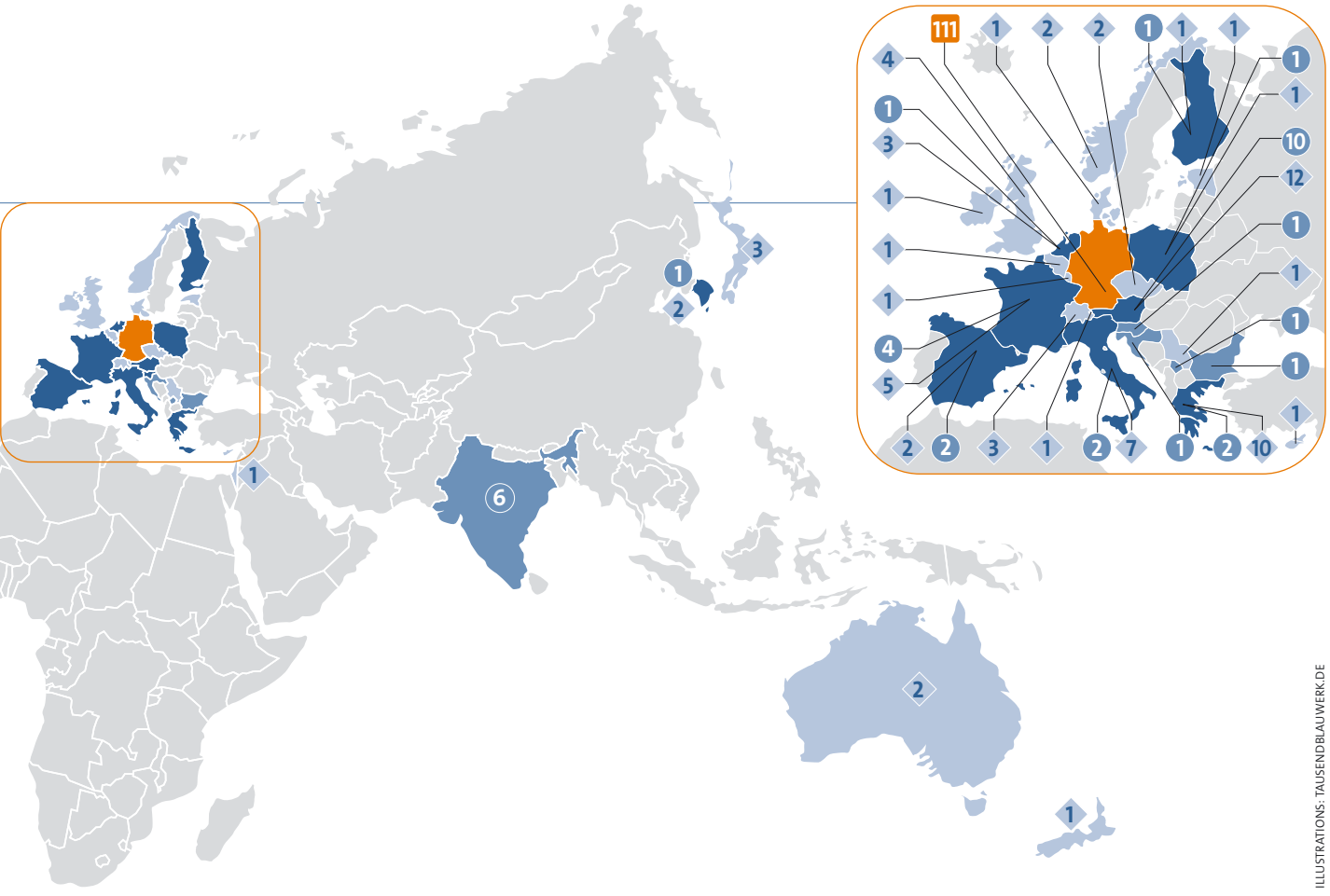
Doctorates

3

Publications



96



ILLUSTRATIONS: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
ANNUAL REPORT
2024

RI CODE
Research Institute
Cyber Defence
Universität der Bundeswehr München

Preface by the President

In an increasingly interconnected world characterized by geopolitical tensions and the rapid development of artificial intelligence, cyber security is one of the greatest challenges of our time. The number of cyberattacks on critical infrastructure, businesses and individuals has grown and requires preventive measures and innovative solutions. In uncertain times like these, it is essential to advance research in the field of cyber security and develop new technologies. With its interdisciplinary fundamental and application-oriented research in the fields of cyber defense, smart data and quantum technology, CODE makes a direct contribution to society and the Bundeswehr and is therefore a key component of our "Security and Sustainability in Technology and Society" profile.

CODE has been conducting successful research at the national and international level for over a decade. In 2024, numerous projects were again carried out and further developed with various partners. Theory and practice were combined to transfer research results into practical applications.

Since 2015, CODE has been working with the Bavarian State Criminal Police Office (BLKA), conducting cyber range training for BLKA personnel and the Bavarian State Office for Information Security (LSI), among others. A cooperation agreement was signed at the end of September 2024 to further strengthen the long-standing and successful collaboration with the BLKA. The particular purpose of the close coordination between the BLKA and UniBw M is to specify requirements and research needs for civil security and develop applications for civil security in projects at the national and international level.

A major success for UniBw M in 2024 was that we were the only German accelerator to be selected for the NATO DIANA program with our Palladion Defence Accelerator. In this program, which offers start-ups access to first-class research and testing facilities, CODE is already participating as a test center and fits perfectly into the innovation ecosystem of UniBw M. The test center is organized jointly with IBM Germany and institutes of the Fraunhofer-Gesellschaft and focuses on innovations in the field of quantum technologies.

CODE is helping to make Germany and the world a safer place by developing innovative solutions for the challenges of tomorrow and strengthening our digital resilience. I would like to congratulate the entire institute on another successful year! You can look forward to interesting insights into the world of cyber security!

With best wishes,

Prof. Dr. mont. Dr.-Ing. habil. Eva-Maria Kern, MBA
President of the University of the Bundeswehr Munich


Wolfgang Hommel, Marcus Knüpfer, Michaela Geierhos

Dear Readers,

The Research Institute CODE at the University of the Bundeswehr Munich combines both basic and application-oriented research with university teaching for future specialists and future leaders of the Bundeswehr and selected federal authorities. Technically exciting and socially and militarily relevant innovations and further developments in our subject areas of cyber defense, machine learning and quantum technologies motivate an in-depth understanding of technology and lifelong learning at the working level, but also at the management and decision-making level, which is also reflected in our continuing education programs.

In 2024, we were delighted with the reaccreditation of our Master's degree course in cyber security, including praise for its content from the external experts, and the further intensified use of our Cyber Range, for example as part of the two-week CYBER PHOENIX, demonstrates our role as a practical partner for training and further qualification.

As established over the last few years, this annual report focuses on our research groups and their projects. It provides you with an insight and overview of the public part of our fields of activity and shows you contact persons and their expertise, which we want to continue to develop and apply in close cooperation with you.

Our report also summarizes other characteristic highlights of the year 2024. For example, the 10th CODE Capture The Flag event took place this year as a small anniversary under the motto "Predator–Threat Hunting", for which the best 20 teams gathered on campus for a weekend. As part of dtec.bw's first annual conference, we had the opportunity to present selected projects and their interim results.

We were also able to contribute to further development at a professional and political level as part of larger events organized by CODE, such as the conference of the German Federal Ministry of Education and Research (BMBF) umbrella project Quantum Communication (SQuaD) and the Board Meeting and Networking Day of the European Cybersecurity Competence Center (ECCC).

We wish you a stimulating read and look forward to further cooperation and joint activities!

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Management of the Research Institute CODE

FIG.: UNIBW M; A. WAGENER FOTOGRAFIE

Contents

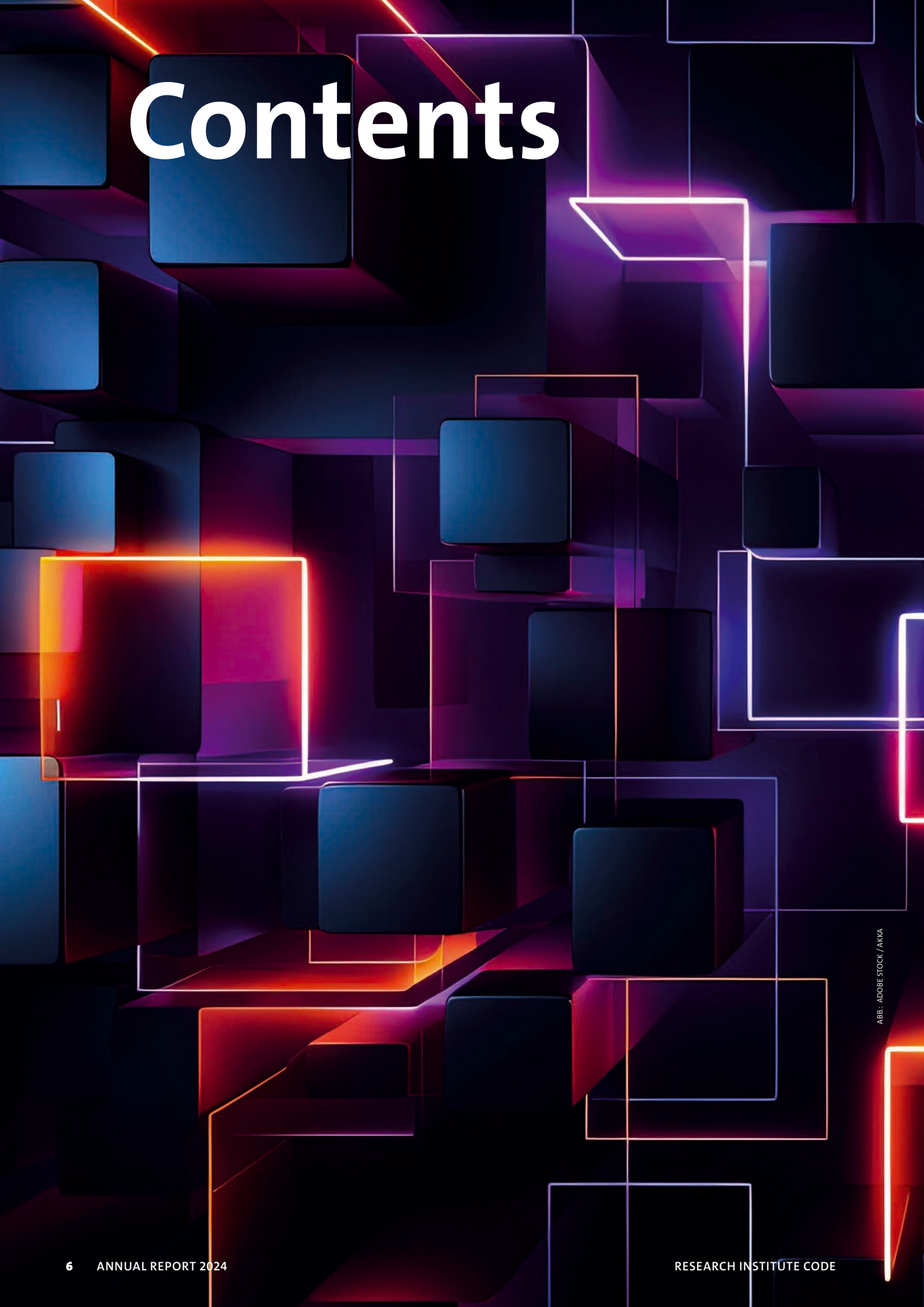


ABB.: ADOBE STOCK / AKKA

Highlights
From the Institute

Research
Portraits and Projects

Further Research Groups and Projects

Cooperations
Germany and the World

Young Science
Offers and Opportunities

Addendum
Publications and Activities

Organizational Structure

Categories

OUR MISSION STATEMENT

FIG.: ADOBE STOCK / STNAZKUL

The Research Institute CODE is a central scientific institution of the University of the Bundeswehr Munich. We use our expertise for the benefit of society and the Bundeswehr and contribute to making Germany a bit safer through innovations in the field of cyber/IT.

Three key areas are the focus of our activities:

- **Research and technology development**
- **Knowledge transfer and consulting for decision-makers**
- **Education and training**

We conduct both basic and applied research as well as technology development in the fields of cyber defense, smart data, and quantum technology. Our work focuses on the concrete and perspective benefits for society and the Bundeswehr. Due to our close ties with the Bundeswehr's CIDS (Cyber and Information Domain Service) military branch, we are in a unique position to develop solutions for current and future challenges in the CIDS domain through research in a secure environment.

Our goal is to research technical innovations and concepts for the protection of data, software, and systems in a holistic and interdisciplinary manner. In particular, we emphasize the development of application-oriented technologies and the acceptance of secure technologies by society. To this end, we work closely with the Bundeswehr, government agencies, research institutions, and industry so that our partners can transfer new research findings and technologies into practice in a way that adds value.

We are open to scientific discourse and pursue long-term cooperations. With the broad competencies of our professorships and research groups, we provide advice to decision-makers from the Bundeswehr and politics and promote knowledge transfer. Our scientific advisory board actively supports RI CODE in its strategic development with its technical expertise.

We offer an optimal framework for education and training. Our IT infrastructure allows research and training at the highest level. In teaching, we prepare students at the University of the Bundeswehr Munich for the challenges of their professional lives and provide practical training for members of the Bundeswehr and Cyber Reserve in our modern Cyber Range. Direct access to quantum computers enables us today to find innovative solutions for the challenges of tomorrow.

We stand by our responsibility and role model function to work together with our partners and, above all, the Bundeswehr to protect a free democratic society. Every day, we are working to make a significant contribution to protecting against the dangers in cyber and information space, and we are prepared to be measured against this. ■

FIG.: ADOBE STOCK / PINKEYES

Highlights

From the Institute

With more than 500 participants, the CODE Annual Conference 2024 set a new visitor record. Selected companies presented themselves to the expert audience at the accompanying exhibition.

Report on the CODE Annual Conference 2024

AI threats and opportunities

“Together with AI against new cyber threats” was the motto of the CODE Annual Conference 2024. Participants from research, industry and the Bundeswehr took part in the two-day event on July 10 and 11 on the campus of the University of the Bundeswehr Munich (UniBw M). With more than 500 participants, it was the largest event for CODE to date. The numerous high-ranking guests included Dr. Reinhard Brandl, Member of the German Bundestag, Bavaria’s Digital Minister Dr. Fabian Mehring and Lieutenant General Michael Vetter.

THE CONFERENCE PROGRAM was opened with welcoming speeches by Prof. Dr. Uwe M. Borghoff, Vice President of UniBw M, and Prof. Dr. Michaela Geierhos, Technical Director of the Research Institute CODE. This was followed by the keynote speech by Brigadier General Michael Volkmer. The Commander of the ZDigBw (Bundeswehr Centre for Digitalisation and Cyber and Information Domain Capability Development) reported on the current efforts of the ZDigBw to provide a basic infrastructure for the digitization of the armed forces by 2029. Prof. Dr. Norbert Pohlmann, Professor of Information Security and Managing Director of the Institute for Internet Security (if(is)) at the Westphalian University of Applied Sciences Gelsenkirchen, shed light on the topic of "IT Security and Artificial Intelligence".

After the opening presentations and a break, the afternoon program continued with three presentations on the topic of artificial intelligence. Prof. Dr. Christian Hummert, Research and Managing Director of the Cyberagentur (Cyber Agency), presented the Cyberagentur's AI perspectives and funding activities in his lecture "Security for AI". The "Impact of AI on the cyber threat landscape" was the topic of the presentation by Dr. Christoph Martin from the BSI (German Federal Office for Information Security). In particular, he warned of the increasing maturity of social engineering attacks in text, sound, image and video. Malware is now also being optimized with the help of AI to such an extent that it can no longer be detected. Andrea Martin from IBM Deutschland GmbH posed the question "Artificial intelligence and cyberspace—who benefits more: defenders or attackers?".

Exhibition and workshops

The annual conference was accompanied by a two-day exhibition. On both days, selected IT companies were able to present themselves and provide information about the latest developments in the cyber sector. During the breaks in the program, guests also had the opportunity to listen to presentations on current cyber security topics in the Coffee Corner.

The rest of the afternoon was dedicated to workshops. From quantum technologies to AI—a wide range of topics awaited the participants in a total of five parallel workshops.

At the end of the first day of the event, Susanne Dehmel, member of the management board of the digital association BITKOM e.V., shed light on the topic of cyber security from a business perspective in her presentation. Her plea for stronger networking between the players in this field met with great approval from the audience. This was then immediately followed up at the get-together with which the organizers brought the first day to a close.

Among the high-level speakers at the CODE Annual Conference were Dr. Reinhard Brandl (right), Member of the German Bundestag, and Bavarian State Minister for Digital Affairs, Dr. Fabian Mehring (2nd from right). They were welcomed by Executive Director Prof. Dr. Wolfgang Hommel and Technical Director Prof. Dr. Michaela Geierhos.

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE

Political keynotes and innovation conference

The second day of the Annual Conference was opened by CODE's Executive Director Prof. Dr. Wolfgang Hommel. He welcomed the high-ranking guests from politics and the Bundeswehr and gave an overview of the recent developments at RI CODE. He was followed by Lieutenant General Michael Vetter. In his keynote speech, the head of the cyber/IT department and Chief Information Officer at the BMVg (Federal Ministry of Defense) spoke about "Software-defined defense as a new paradigm for the capability development of the armed forces". In his speech, Dr. Reinhard Brandl, Member of the German Bundestag, presented a ten-point program with which the turnaround can also be implemented in cyber defence. The Bavarian State Minister for Digital Affairs, Dr. Fabian Mehring, also addressed the conference participants on the topic of cyber security and the challenges in this area. He warned that the mistakes of the past should not be repeated and new dependencies should not be created in the course of digitalization, creating new dependencies that could lead to blackmail. To this end, it is particularly important to protect sovereignty over one's own data, but also to integrate the topic of cyber security more strongly into people's everyday lives.

The morning's political keynotes were followed by the Cyber/IT Innovation Conference. With this ideas competition, the Bundeswehr aims to break new ground in identifying IT innovations for possible use in the BMVg's business area. More than 30 applications were received this year, from which an expert jury selected the eight best concepts in advance and invited them to the conference. The eight finalists presented their ideas to the expert audience in seven-minute short pitches. These ranged from highly secure routing architectures in Quantum Key Distribution networks to innovative sensor modules for semi-autonomous battlefield reconnaissance and transportable quantum computers. Guests also had the opportunity to get in touch with the speakers during the subsequent meet-the-speakers session. In the end, Simon Klink from SE3 Labs GmbH came out on top. His idea of real-time 3D reconnaissance using autonomous drones (UAVs) with an AI cockpit won over the expert jury and earned him the prize money of €15,000. Second and third place went to João Schneider, University of Giessen ("The VERITAS system 'Hornet': Seamless situational aware-

Group photo with the participants of the innovation conference (from left to right): (top row): Andreas Walbrodt (Enclaive GmbH), Prof. Dr. Wolfgang Hommel (Executive Director RI CODE), Brigadier general Armin Fleischmann (Head of subdepartment CIT I at the BMVg), Dr. Wolfgang Meißner (ARQUE Systems GmbH), Simon Klenk (SE3 Labs GmbH), João Schneider (Universität Gießen), (bottom row): Dr.-Ing. Emmanuel Stapf (SANCTUARY Systems GmbH), Peter Horoschenkoff (Rohde & Schwarz Cybersecurity / TU Munich), Hussein Hasso (Fraunhofer FKIE), Dr.-Ing. Felix Heilemann (Sagio GmbH).

Panel discussion (f.l.t.r.): Felix Broßmann (panel moderator), Miriam Schnürer, Dr. Pascal van Overloop, Victoria Toriser, Cora Lisa Perner and Dr. Kai Martius.

ness based on AI-supported sensor data evaluation“) and Dr. Markus Adrian Peter Beckers, ARQUE Systems GmbH (“Novel chip architecture for a transportable quantum computer for direct use in conflict situations for various applications”). The remaining finalists were also awarded a prize of €1,000.

Science track and panel discussion

The afternoon program started after a break with the science track. Two scientists gave the audience insights into their current research. PD Dr. Sabine Wölk from the German Aerospace Center (DLR) spoke about the risk and potential of quantum computing. Prof. Dr. Daniel Slamanig and Prof. Dr. Marta Gomez-Barrero, both at RI CODE since the end of 2023, presented their research on “Cryptography and AI” and “Biometric Recognition”.

The afternoon continued with the presentations “Technological threats from the air drones, swarms and smart dust as risks for critical infrastructures” by Miriam Schnürer, BKSI (Federal Association for the Protection of Critical Infrastructures), and “Cyber & AI in the Russian war” by Volker Kozok, Network for Cyber Intelligence.

In the closing panel discussion, experts from the military and industry talked about “Innovation in the corset—AI security in Germany”. Speakers included Dr. Kai Martius, Member of the Management Board / Chief Technology Officer (secunet Security Networks AG), Miriam Schnürer (Member of the Management Board, BKSI e.V.), Cora Lisa Perner (R&T Cybersecurity, Airbus Defence and Space), Victoria Toriser (Cyber Basics and Innovation, Austrian Armed Forces) and Dr. Pascal van Overloop (Industry Advisor Defense & Intelligence at Microsoft Deutschland GmbH). The discussion was moderated by Felix Broßmann (SKAD AG).

The closing remarks by CODE’s Executive Director Prof. Dr. Wolfgang Hommel concluded the lecture program of the CODE Annual Conference 2024. With 540 participants, it was the largest annual conference for CODE to date. He thanked all participants and supporters for their great commitment and took the opportunity to invite to the next conference on July 8 and 9, 2025. ■

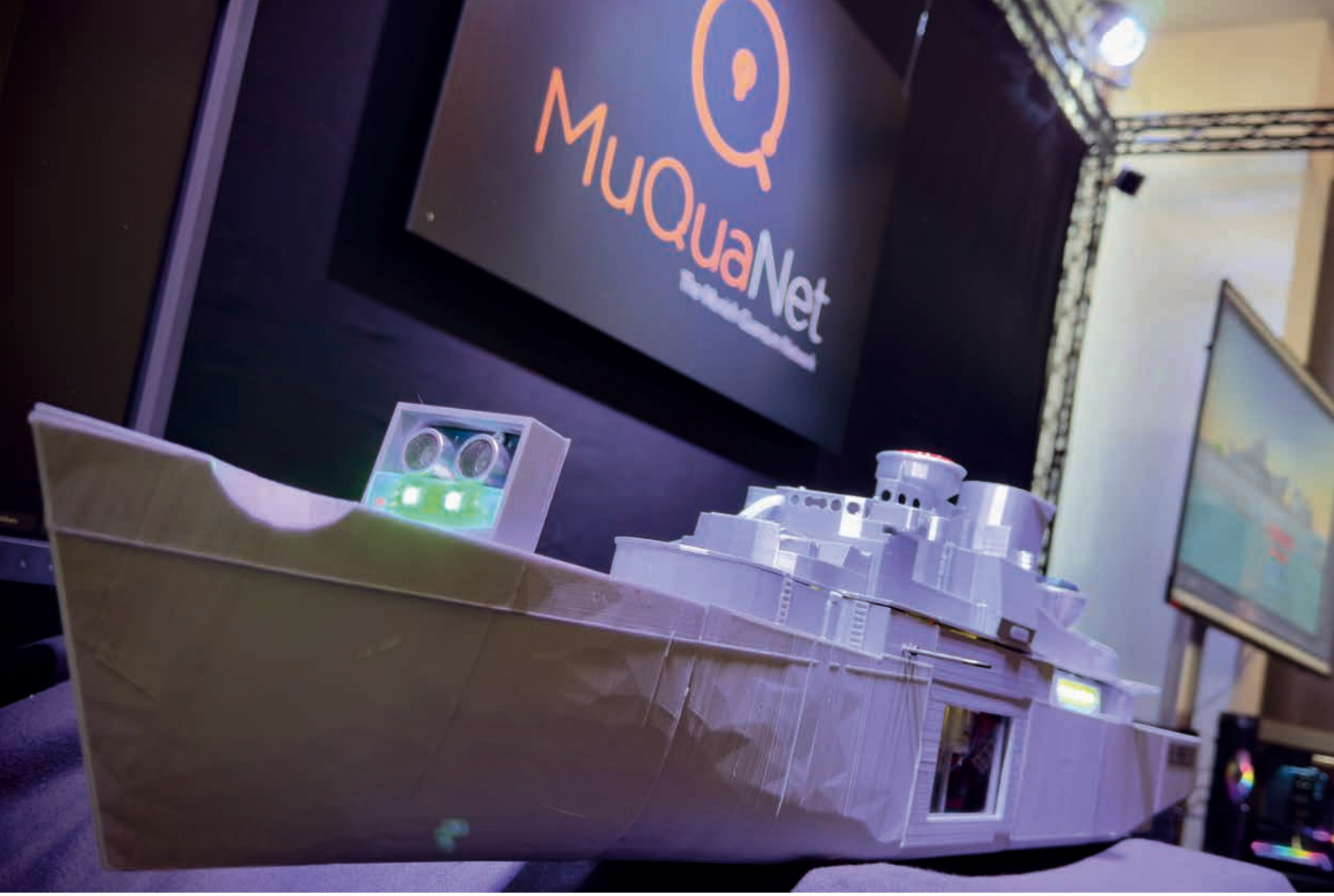
More information on the CODE Annual Conference

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (2)



Report on the dtec.bw Annual Conference 2024

Hands-on Future Technology

At the first annual conference of the Bundeswehr Centre for Digitization and Technology Research on 17 and 18 September 2024, CODE presented two future-oriented research projects to an expert audience.

OVER 600 GUESTS from Bundeswehr, science, industry and start-ups were drawn to the campus of the University of the Bundeswehr Munich (UniBw M) in mid-September 2024. Under the motto "Research with added value for all dimensions", the Bundeswehr Centre for Digitalization and Technology Research (dtec.bw) invited guests to Neubiberg to present its wide range of research projects to the specialist audience. In a packed program, numerous projects from the dimensions of air, land, sea, human, space and cyber, which are being worked on at the Bundeswehr universities in Hamburg and Munich, were presented during the two-day event. The Research Institute CODE also presented two of its six dtec.bw-funded projects.

With a showcase, the MuQuaNet team impressively demonstrated one of many possible application scenarios for quantum-secure encrypted data transmission.

Quantum-safe communication in application

The conference began with a ceremonial opening by the President of UniBw M, Prof. Dr. Eva-Maria Kern, and greetings from high-ranking representatives of the Federal Ministry of Defense. Prof. Dr. Wolfgang Hommel presented the Munich Quantum Network (MuQuaNet) research project to the numerous guests in the Audimax as a selected project from the cyber research dimension. The aim of the project is to develop, build and operate a quantum-safe communication network for research and evaluation with UniBw M at its core and to make it available to other research institutions, authorities and military units. Built from various components, it is intended to prepare for seamless integration into existing network communication, demonstrate the wide range of possible applications and serve as a blueprint for the construction of customized, highly secure communication networks. The employees at the MuQuaNet stand in the foyer were later delighted with the high level of interest, where they provided exciting insights into their research work and demonstrated an impressive use case for the technology showing a quantum-secure encrypted virtual reality remote maintenance environment.

Technical components for quantum-safe encryption.

Blackout communication: stay informed in the event of a desaster

On the second day of the dtec.bw Annual Conference, visitors had the opportunity to take various focus tours on the university campus and experience the various dtec.bw-funded projects up close. In addition to MuQuaNet, the Resilient Operation of LoRa Networks (ROLORAN) project also presented its work. At their booth, they showed, among other things, an infrastructure for blackout crisis communication, as it is needed after severe natural disasters, for example. The LoRa radio technology used here is not only particularly energy- and cost-efficient, but is also characterized by its long range. A corresponding system is to be set up and evaluated in the municipality of Neuhaus (Carinthia, Austria) as of 2025.

The ROLORAN project team led by Prof. Hommel (r.) presented a self-developed system for blackout crisis communication.

The dtec.bw annual conference 2024 clearly showed how many achievements have already been made in the first funding phase (until the end of 2024) and how closely the universities of the Bundeswehr are working together, both with each other and with external partners, to transfer research results into practical applications. The next annual conference will take place in Hamburg in September 2025.

dtec.bw is funded by the European Union – NextGenerationEU.

dtec.bw

Funded by the European Union
NextGenerationEU

More Information (in German)

www.dtecbw.de

go.unibw.de/roloran

go.unibw.de/muquanet

ALL FIG.: RI CODE / B. BELLGRAU

LSI President Bernd Geisler (r.) visited the training participants at RI CODE.

BLKA and LSI Practice at RI CODE

Teaming up

Members of the Bavarian State Criminal Police Office (BLKA) and the Bavarian State Office for Information Security (LSI) took part in cyber training at the RI CODE's Cyber Range in March. LSI President Bernd Geisler and Vice President Dr. Thomas Kaiser as well as representatives of the BLKA visited the twelve participants on site and took the opportunity to talk to CODE Director Prof. Dr. Wolfgang Hommel.

A key aspect of the training was the close cooperation within the mixed team.

ON MARCH 21 AND 22, BLKA and LSI personnel trained together at the RI CODE's Cyber Range to combat cyberattacks. The twelve active participants were challenged in a realistic scenario. The aim was to practice the response to a complex cyberattack on a hospital.

Real-life challenge: an advanced persistent threat (APT)

In the "InTime" scenario, the participants were confronted with a threatening situation: A hospital's IT system had been encrypted by ransomware. This had a catastrophic impact on operations and patient safety. However, it was not just a simple one-stage attack. The attack was a so-called advanced persistent threat (APT), in which the attacker not only gains access to the network, but also continues to operate inconspicuously by disguising itself and taking over other systems. The attacker also used evasion techniques to bypass security software.

The fact that the participants were not provided with any additional information, such as network maps, was particularly challenging. All relevant information had to be obtained by the participants themselves, either by interviewing the situation actors or using other investigative methods. This reflects the reality in which forensic scientists and IT experts often have to work with incomplete information. Real vulnerabilities were exploited to make the attack as authentic as possible. Three vulnerabilities from 2021 were linked together by the training instructors to allow the fictitious attackers access to the system. This type of approach also gave participants the opportunity to sharpen their skills in identifying and fixing vulnerabilities.

Practical exercise and a tough challenge: reacting to the attack and forensic analysis

The training began with simple exercises in which the participants were introduced to the system and tools used. The main scenario, which simulated the APT attack, then started at midday on the first day of training and ran until the end of the second day. During this time, the investigators not only had to deal with the attack itself, but also carry out forensic analyses and understand the processes in the hospital network.

Close collaboration within the mixed team was a key aspect of the training. By sharing expertise and resources, the participants were able to gain valuable insights and further develop their skills in dealing with cyberattacks. Such exercises are crucial to ensure the safety of the digital infrastructure in the future and to further strengthen the authorities' ability to respond in critical situations.

In a meeting held parallel to the exercise, high-ranking representatives from LSI, BLKA and RI CODE discussed the further need for Cyber Range-based training and opportunities for closer cooperation between the three institutions in the future. ■

ALL FIG.: RI CODE / B. BELLGRAU

Talked about the further need for Cyber Range-based training and the opportunities for closer cooperation (f.l.t.r.): Vice President Dr. Thomas Kaiser (LSI), Executive Director Prof. Dr. Wolfgang Hommel (RI CODE), President Bernd Geisler (LSI), Criminal Director Dieter Hausberger (BLKA) and Chief Criminal Director Simone Lang (BLKA).

IBM's quantum chips are at the heart of its vision for a quantum-centric supercomputer.

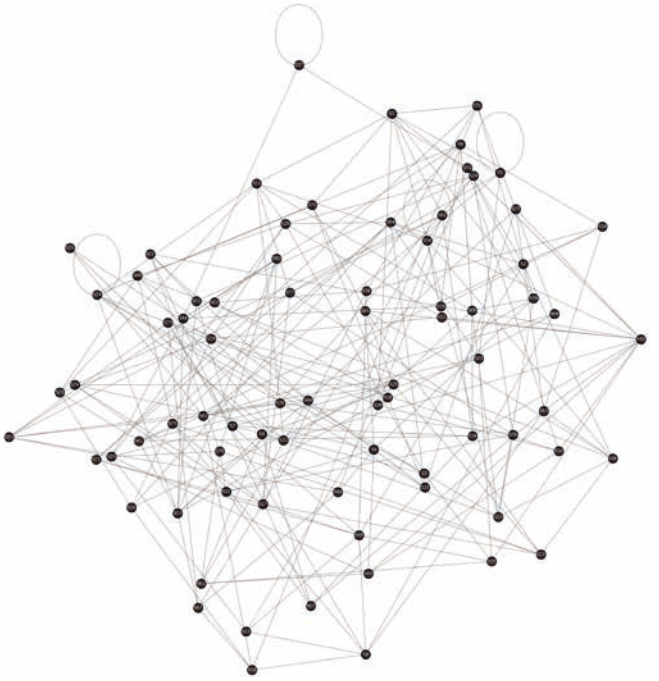
Decision-Making Under Uncertainty and Optimization

Fundamental research paves the way for practical applications

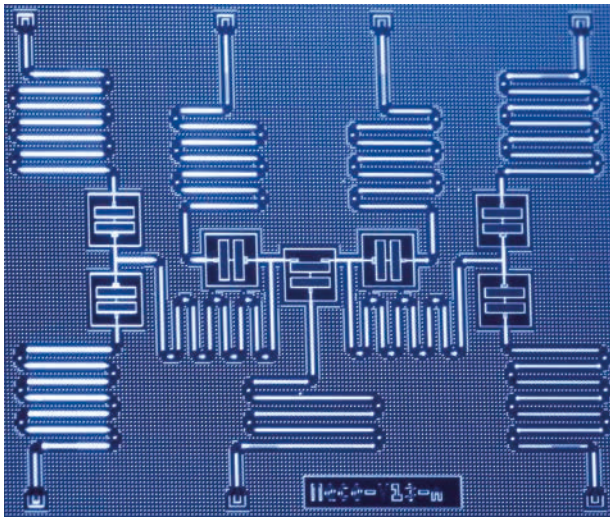
Quantum technologies are transforming the fields of computing, sensing and communication through three key components: quantum computers, which perform some complex calculations at previously unreachable rates; quantum sensors, which detect physical phenomena with extreme accuracy; and quantum networks, which securely connect quantum systems over long distances. Together, these elements provide the basis for innovative (quantum) information processing.

QUANTUM INFORMATION science builds on fundamental research to discover practical applications and identify relevant use cases. By applying the core principles of quantum mechanics, researchers can drive innovation in computing, communication and sensing. This deep understanding of the scientific foundations facilitates the translation of theoretical quantum concepts into real-world applications and simulations on testbeds such as the IBM Quantum Chip.

Quantum computing offers enormous potential for realizing advantages in computing. An essential requirement for the efficiency of a quantum algorithm is the targeted use of certain quantum properties such as superposition, interference, entanglement and indeterminacy. Classical algorithms were developed both theoretically and empirically, with empirical methods sometimes leading to theoretical insights later. In contrast, the development of quantum algorithms was primarily theoretical due to the limited availability of hardware, but this changed with the advent of technologies such as gate-based quantum computers with dozens of qubits that can execute complex circuits that are already reaching the limits of the simulation capabilities of classical computers.



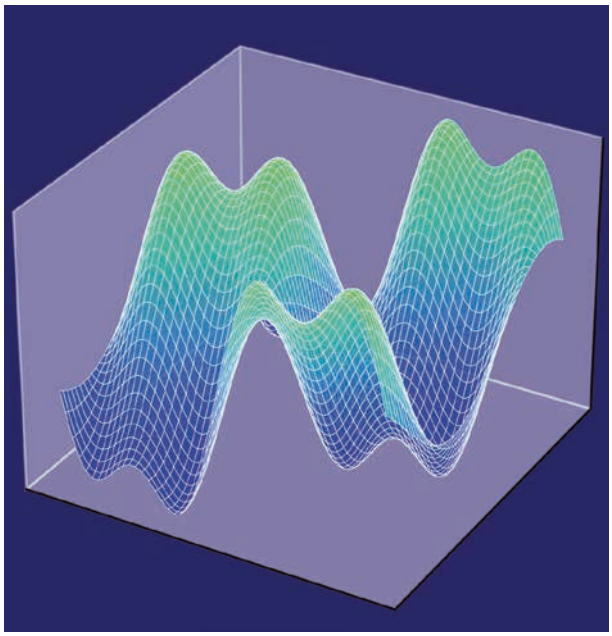
Network with Markov processes.



Quantum computers as a test environment for quantum information processing.

At RI CODE, one of the applications of quantum computing is to solve complex decision problems under uncertainty, which often exceed the capabilities of classical computers. Quantum computing paradigms are used to improve the management of complex stochastic models. A particular focus is on multidimensional Markov processes, which are crucial for decision-making under uncertainty. Quantum computing uses quantum mechanics to process information more efficiently than classical systems and offers innovative solutions to these challenges.

FIG.: IBM; IBM RESEARCH / SCIENCE PHOTO LIBRARY; CHATGPT



Exemplary visualization of an optimization.

Another research focus at RI CODE is on quantum walk algorithms, which represent a quantum mechanical counterpart to classical random walks and are of central importance for the development of quantum algorithms. They provide a framework that uses quantum mechanics to explore complex networks and probability distributions. When making decisions under uncertainty, quantum walks can provide a significant computational advantage.

Quantum walks significantly increase the efficiency of search algorithms on specific graphs and data structures, accelerate the identification of critical factors within complex datasets and improve strategic decision-making processes.

Quantum walks and quantum optimization are important techniques in quantum computing to tackle complex computational challenges. Quantum walks are characterized by their ability to quickly navigate through large solution spaces to find optimal or near-optimal solutions in scenarios with multiple complex and uncertain variables. These techniques are used to solve certain optimization problems in various fields such as logistics, machine learning and engineering more efficiently than with classical computing.

Furthermore, quantum walks are crucial for the **simulation of distributed quantum information in networks**, which is essential for secure quantum communication. This includes detailed modeling of quantum states, network components and interactions, supported by robust quantum software tools. As quantum computing technology advances, the ability to accurately simulate and optimize quantum networks becomes increasingly critical for the development of practical quantum communication systems and protocols.

Quantum algorithms for Markov processes use the principles of quantum mechanics to efficiently analyze and simulate systems with Markovian dynamics and offer potential computational advantages over classical approaches. These algorithms are ideal for scenarios in which the dynamics follow Markov processes. Quantum walks, a key technique in this area, enable the simulation of quantum system evolutions that follow Markovian rules and effectively apply quantum dynamics simulations to such systems. Quantum walks have the potential to improve decision-making processes under uncertainty by providing a fundamentally new way of computing, exploring and predicting complex systems.

Since the **inherent noise in quantum systems** can significantly affect computational accuracy, error reduction is of essential importance. Two important techniques in this area are probabilistic error compensation and zero noise extrapolation. These strategies help to improve the reliability of quantum computations without having to resort to full quantum error correction, which requires considerable resources.

Noise visualization.

Probabilistic Error Cancellation: This approach involves a sophisticated method in which errors in quantum operations are modeled and then compensated for by applying a quasi-likelihood-based representation of the inverse noise process. This method relies heavily on an accurate noise model and involves adjusting the results based on the probabilities of different error processes.

Zero Noise Extrapolation: This technique takes a more empirical approach by manipulating the noise level that affects the system. By running the same quantum circuits at different controlled noise levels and extrapolating the results, it is possible to estimate what the results would look like in an ideal noise-free environment. This technique does not require such detailed knowledge of the noise model, but depends crucially

on the ability to scale the noise accurately and on the adequacy of the extrapolation model used.

Significant progress has already been made in the field of **quantum error correction**. Current techniques are intermediate solutions that enable more accurate calculations on Noisy Intermediate-Scale Quantum (NISQ) devices. As quantum technology advances, more sophisticated and resource-efficient error correction methods are likely to be developed. These advances could potentially enable longer, more complex and more accurate quantum computations. In addition, the integration of error minimization techniques with advanced quantum error correction protocols could pave the way for the next generation of quantum computers. This integration could enable practical quantum computing at a scale and accuracy unachievable with current technologies. Progress in this area will depend not only on theoretical advances, but also on improvements in quantum hardware, such as better coherence of qubits, improved quantum gates, and more effective noise characterization and control. These developments will help to achieve the long-term goal of a fully error-corrected quantum computer and open up new possibilities in various fields such as cryptography, materials science and simulation of complex systems.

At RI CODE, **teaching materials** are developed to introduce students to the practical and theoretical aspects of quantum computing. The exploration of these approaches includes both theoretical studies and practical prototypical implementations. This two-pronged approach helps students to understand complex concepts and apply them in real-world scenarios. In addition, the course material is enriched by experiments with quantum computers and the semantics of quantum circuits, supported by computational symbolic calculations using tools such as computer algebra systems and theoretical models such as the ZX calculus. This comprehensive educational framework fosters a deeper understanding and facilitates automated thinking in quantum programming, preparing students for further studies and research in quantum computing.

As quantum technologies are rapidly evolving through improvements in quantum hardware combined with more sophisticated algorithms, new applications are opening up, such as decision making under uncertainty and optimization. In addition, interdisciplinary collaboration between quantum physicists, data scientists and computer scientists will be crucial to tailor quantum solutions for specific decision problems and thus maximize the quantum advantage. Although quantum computing is still in its early stages, it promises to transform the way complex decisions are made under uncertainty.

FIG.: CHATGPT (2)

IBM Innovation Center

AS AN IBM Innovation Center, the RI CODE at the University of the Bundeswehr Munich has had access to the IBM quantum computing infrastructure since 2018. The current availability of low-noise quantum computers (up to 156 qubits) enables scientists to test quantum algorithms, heuristics, error correction and error mitigation schemes, as well as perform experiments to explore quantum information processing and simulate quantum networks and quantum sensors. Research at RI CODE focuses on the development of algorithms and applications in the areas of quantum optimization, quantum machine learning, quantum simulation and quantum error correction.

Furthermore, quantum walk algorithms are developed and implemented on IBM quantum computers using circuit optimization and error reduction techniques. The quantum computers are programmed with the software development kit “Qiskit” at circuit and algorithm level, and corresponding experiments are carried out. At the same time, the teaching program for students will be further expanded and lectures, laboratory practices and workshops on quantum information processing will be offered.

Latest publications of the Quantum Innovation Center

YIN, R., WANG, Q., TORNOW, S., BARKAI, E.: Restart uncertainty relation for monitored quantum dynamics. PNAS 122 (1), e2402912121 ,(2025).

DEVRA, A., VAN DAMME, L., ENDE, F. V., MALVETTI, E., GLASER, S. J.: Theory and Experimental Demonstration of Wigner Tomography of Unknown Unitary Quantum Gates. arXiv preprint arXiv:2411.05404, (2024).

ABBAS, A., AMBAINIS, A., AUGUSTINO, B., BÄRTSCHI, A., BUHRMAN, H., COFFRIN, C. et al.: Challenges and opportunities in quantum optimization, Nature Reviews Physics, 1-18 (2024).

WANG, Q., REN, S., YIN, R., ZIEGLER, K., BARKAI, E., TORNOW, S. : First Hitting Times on a Quantum Computer: Tracking vs. Local Monitoring, Topological Effects, and Dark States Entropy 26 (10), 869 (2024).

TORNOW, S., ZIEGLER, K.: Measurement-induced quantum walks on an IBM quantum computer. Physical Review Research 5 (3), 033089, (2024).

OECD GFTech focus group on quantum technologies: A quantum technologies policy primer OECD DIGITAL ECONOMY PAPERS January 2025 No. 371

SQuaD quantum communication workshop at the UniBw M

For the first time, the SQuaD workshop, one of the most important conferences in the field of quantum communication, took place on the university campus in Neubiberg from April 16 to 18, 2024. Top scientists, researchers and experts from industry came together to discuss the latest advances and research findings in the field of quantum communication.

QUANTUM COMMUNICATION is a key technology for the security of digital infrastructures in our society. The conference, part of the projects "SQuaD" (Umbrella Project Quantum Communication in Germany) and "MuQuaNet" (Munich Quantum Network), brought together funding projects of the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of Defense (BMVg) with their experts and networks for the first time. In her opening speech, the President of the University of the Bundeswehr Munich (UniBw M), Prof. Dr. Eva-Maria Kern, emphasized the high relevance of networking and cooperation in the context of current challenges and that FI CODE has contributed significantly to the development of an ecosystem around the topic of quantum communication. Prof. Wolfgang Hommel, Executive Director of FI CODE, also underlined the great importance of secure quantum communication for society as a whole.

In his talk, Prof. Dr. Wolfgang Hommel emphasized the importance of quantum-safe communication for society as a whole.

FIG.: UNIBW M / SIEBOLD

Quantum communication is a key technology

During the two days of the event, a wide range of topics was covered, providing in-depth insights into the current status and future possibilities of quantum communication. Participants had the opportunity to find out about the latest research results in projects such as SQuaD, MuQuaNet, 6G-QuaS and DE-QOR. These projects are also setting international standards in the development of quantum communication networks and technologies.

Another key topic was market developments in the field of quantum key distribution (QKD), a theoretically tap-proof method for the transmission of encryption keys based on the principles of quantum mechanics. The urgency of developing and implementing QKD systems was emphasized in light of the increasing threats posed by advanced and powerful computing technologies such as quantum computers, which can potentially break conventional encryption methods, and an increased threat situation on the European continent.

The importance of quantum communication as a key technology for the security of future communication networks was impressively underlined by the event. The projects SQuaD and MuQuaNet demonstrated the strong commitment and high volume of investments in research and development at both national and international level.

The two projects combine the expertise and know-how from science and industry to work together on the development of a secure communications infrastructure for the future. This pioneering work is already laying the technological foundations for future quantum communication networks and driving forward the intensive exchange between research institutions and industry in order to find innovative solutions to the challenges of data security in the age of quantum computing. ■

At the NCC network meeting in October, representatives from the 27 EU member states as well as Norway and Iceland came together on the university campus in Neubiberg.

EU cyber security: Network meeting in Neubiberg

As part of the German National Cybersecurity Coordination Center (NCC-DE), the Research Institute CODE (RI CODE) hosted the network meeting of the National Cybersecurity Coordination Centers (NCCs) and the 10th meeting of the Administrative Board of the European Cybersecurity Competence Center (ECCC) from October 9 to 11, 2024 on the campus of the University of the Bundeswehr Munich. The event was organized in cooperation with the Federal Office for Information Security (BSI), the head office of the NCC-DE.

Over the course of the three days, around 120 participants from the 27 EU member states, Norway and Iceland came together on the campus of the University of the Bundeswehr Munich. The first day was opened by Laurie Tanker, Chair of the NCC network. The participants were then welcomed by Luca Tagliaretti, Managing Director of the ECCC, and Prof. Dr. Wolfgang Hommel, Executive Director of RI CODE. In his welcome address, Prof. Hommel highlighted the consortium structure of the NCCs in particular and emphasized the role that RI CODE plays in this context. With its research, RI CODE not only creates additional value for the Bundeswehr, but also for European society as a whole.

The program of the NCC Network Day included presentations by the European Commission, the ECCC and the European Union Agency for Cybersecurity (ENISA), as well as numerous networking sessions where the NCC representatives were able to share their experiences in connection with the implementation of the Digital Europe Programme (DEP) at national level.

At the end of the day, Laurie Tanker from NCC Estonia was confirmed in her position as Chair of the NCC network by the representatives of the National Coordination Centers. Two new deputy network chairs from Luxembourg and Iceland were also elected.

On October 10 and 11, the ECCC Administrative Board met with representatives of the EU member states, Norway and Iceland to discuss and decide on the future direction of the Digital Europe Programme (DEP) for the period 2025 to 2027.

Six working groups were set up to discuss and support the future development of the DEP. ■

Detailed information on the activities of the German NCC can be found online at:

https://nkcs.bund.de/

FIG.: RI CODE / B. BELLGRAU

GOR Chairman Prof. Dr. Alexander Martin (l.) presents the honorary membership to Prof. Dr. Stefan Pickl (r.).

Award for Prof. Dr. Stefan Pickl

At the annual conference of the German Operations Research Society (GOR) in Munich, Prof. Dr. Stefan Pickl was awarded honorary membership. With this recognition, the GOR honors his outstanding commitment as a member of the advisory board and as editor of the society's journal, OR News.

THE 2024 ANNUAL conference of the German Operations Research Society (GOR) took place as a joint event with the Austrian Society for Operations Research (ÖGOR) and the Swiss Operations Research Society (SVOR/ASRO) under the motto "Data, Learning, and Optimization" from September 3 to 6 at the Technical University of Munich.

Recognition for exceptional commitment

A particular highlight was the formal award ceremony for Prof. Dr. Stefan Pickl. During the Opening Ceremony and in the presence of around 700 participants of OR 2024, he was presented with honorary membership by GOR Chairman Prof. Dr. Alexander Martin. The GOR recognized his outstanding and long-standing contributions as chair of the advisory board as well as his dedicated work as editor of the society's journal OR News. This honorary membership is a mark of the highest recognition and is awarded only to individuals with exceptional merit – Prof. Pickl is the 20th and, to date, youngest honorary member of the GOR.

Elected to the National Academy of Science and Engineering acatech

At the end of 2023, Prof. Pickl was also elected to the German National Academy of Science and Engineering (acatech). Through his acatech membership, Prof. Pickl joins a circle of outstanding individuals who contribute to shaping technological innovation in Germany through their scientific excellence and societal impact. He brings particular expertise to the field of "Security," where he advocates for interdisciplinary dialogue between science, technology, and society. ■

Prof. Dr. Stefan Pickl (left) receiving the certificate of appointment in Berlin from the President of acatech, Prof. Dr. Jan Wörner.

FIG.: UNIBW M / S. PICKL; TU MUNICH

First International NATO Summerschool: Decision Making for the Future

Officers make decisions – often under extreme pressure. In the digital age, the foundations for such decisions have fundamentally changed: The amount of available information is constantly increasing, as are the methods used to analyze it – particularly through artificial intelligence. Against this backdrop, the Universität der Bundeswehr München, in cooperation with the NATO Science and Technology Organization (STO), hosted the first NATO Summerschool. The event was organized in partnership with the Research Institute CODE.

Major General (Ret.) Reinhard Wolski (left) spoke about the role of AI in military decision-making.

FIG.: UNIBW M / S. PICKL

UNDER THE MOTTO "Decision Making for the Future," around 40 participants from more than eight nations came together. The event kicked off with a joint barbecue on campus, where Vice President Prof. Dr. Uwe Borghoff and CODE Director Prof. Dr. Michaela Geierhos welcomed the attendees. The academic lead of the NATO Summerschool was Prof. Dr. Stefan Pickl, who developed and organized the conference together with the military co-chair, Colonel Matthias Kinkel from the Bundeswehr Planning Office.

Leadership in times of AI and geopolitical uncertainty

In his opening address, Major General Wolfgang Gäbelein, Head of the Bundeswehr Planning Office, emphasized the importance of NATO's technological and scientific superiority in light of current geopolitical challenges. Despite all advancements in AI, he stressed that humans must always remain accountable. He also referenced the 200th anniversary of the Prussian war game – a nod to the historical dimension of decision-making.

Jackie Eaton from the NATO Joint Analysis and Lessons Learned Centre (JALLC) opened the plenary with a keynote speech on the significance of Operational Analysis within NATO. Prof. Dr. Daniel Nussbaum from the Naval Postgraduate School presented the "Energy" task force he founded. Other contributions included Dr. Zenon Matthews from the Swiss Army Staff on data-driven defense analysis, and Major General (Ret.) Reinhard Wolski on the role of AI in military decision-making.

From wargaming to practice: experiencing decision-making processes

A wargaming exercise conducted by the Bundeswehr Planning Office highlighted practical decision-making processes, complemented by lectures on the development and importance of this method. Other key topics included leadership, ethics, and emerging technologies such as biometrics.

The summer school was framed by two historical anniversaries: the 50th anniversary of the death of Operations Research pioneer Patrick Blackett, and the 80th anniversary of the Stauffenberg assassination attempt. In his closing presentation, Prof. Pickl recalled Blackett's guiding principle: "Always be open to new approaches and embrace interdisciplinary discourse."

The summer school will continue in 2025 in Ankara. More than 60 participants have already registered in advance. ■

FIG.: ADOBE STOCK / ITCHAZNONG

Research

Portraits and Projects

Research at RI CODE

Currently, there are 44 third-party funded projects being carried out in various research groups at the Research Institute CODE. A selection of these projects is described on the following pages. CODE conducts research in three overarching business areas: Cyber Defense, Smart Data, and Quantum Technology.

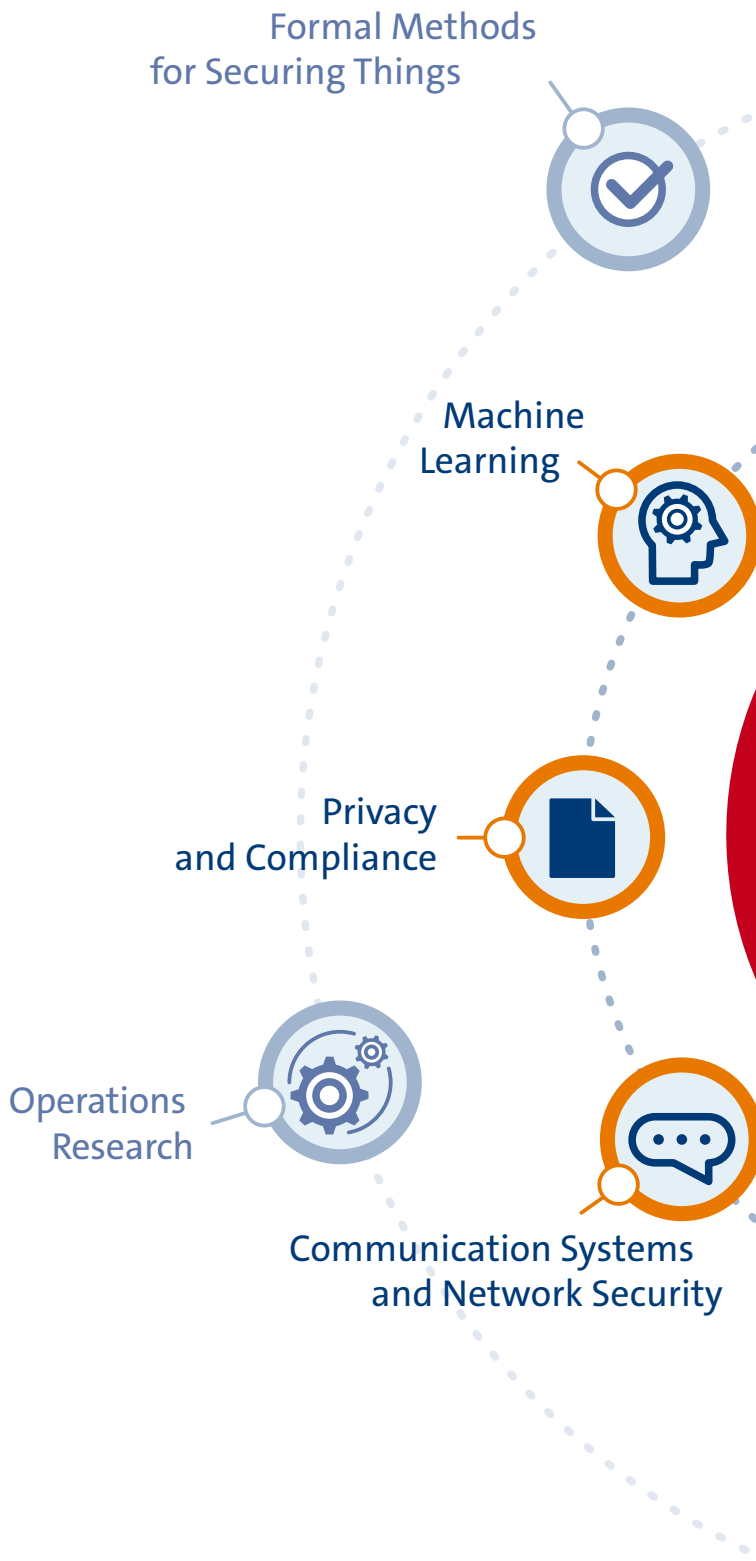
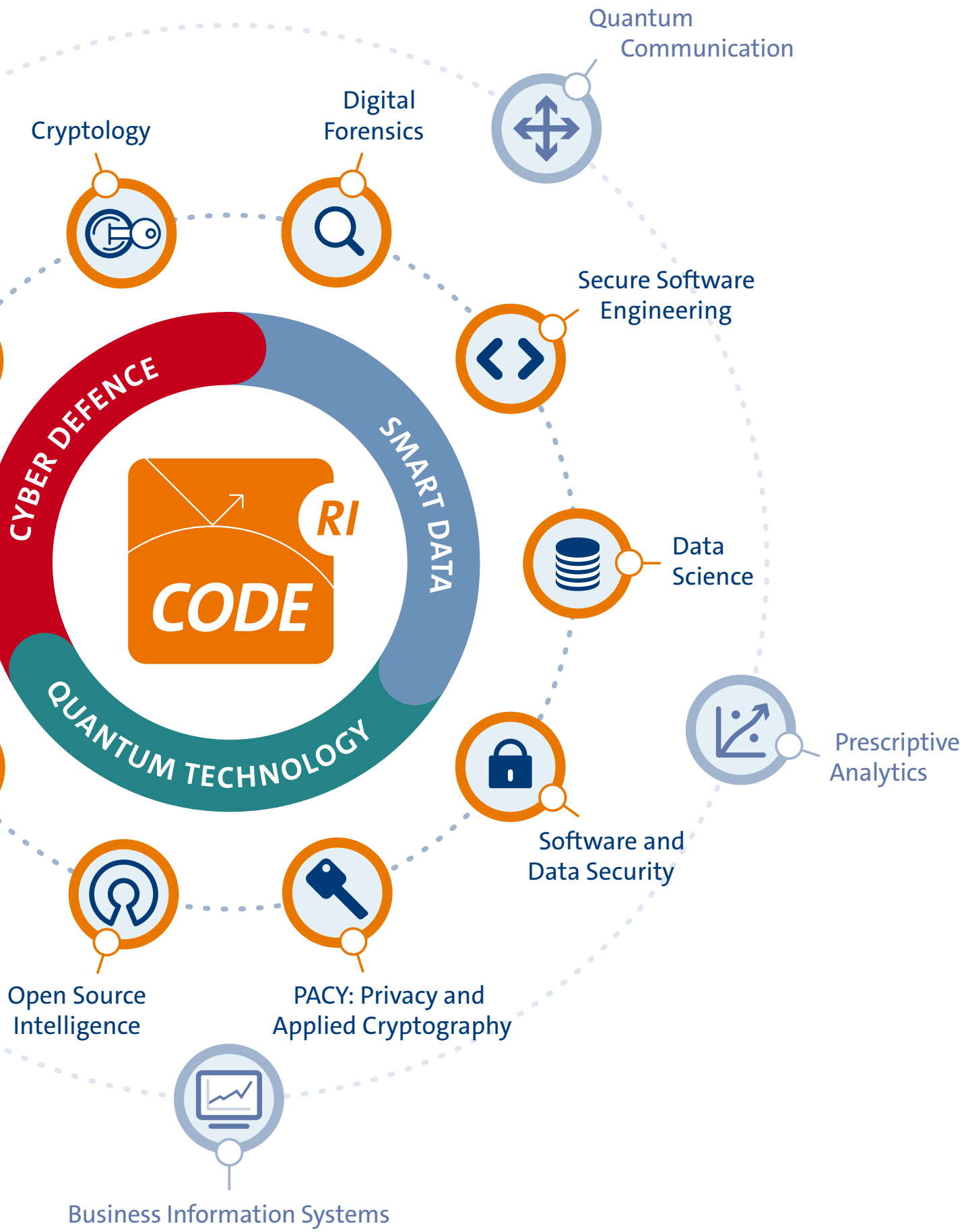


FIG.: TAUSENDBLAUWERK.DE


Quantum Communication
Digital Forensics
Cryptology
Secure Software Engineering
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
RI
CODE
Data Science
Prescriptive Analytics
Software and Data Security
Open Source Intelligence
PACY: Privacy and Applied Cryptography
Business Information Systems

Prof. Dr. Harald Baier

Digital Forensics

Due to increasing digitization and subsequent cybercriminal activities, the need for digital forensics competencies is growing too. The main research areas of the Professorship of Digital Forensics address the handling of bulk data in IT forensic investigations, the generation of synthetic datasets to assess IT forensic tools, anti-forensics, and main memory forensics.

DIGITAL FORENSICS, as the digital equivalent of the classic forensic disciplines, always comes into play when an answer to a question of doubt is sought in connection with an IT system. A case in point would be when a remote-controlled drone is used to transport drugs, but during transport the drone crashes onto the property of a bystander. When called to help, the police take over the drone and are supposed to clarify the questions of doubt as to who was piloting the drone and what routes it was flying. To do this, the supporting IT forensic experts secure the drone's data media, analyze them, and try to provide answers to the questions of doubt.

Seeking access

An IT forensic investigation is associated with numerous challenges, which the Professorship of Digital Forensics deals with. A first important challenge is the question of how data can be secured and analyzed, especially that from innovative IT devices such as drones or cars. The background to this is that these devices often only offer unknown interfaces for access and that data storage is dependent on the manufacturer in terms of partitioning, the file system, and the file format.

Searching for training data

A second important challenge is the accuracy of IT forensic tools, meaning that they should work as specified. This requires standardized test datasets. For these, the digital traces to be detected are known a priori and matched against the detected traces by the respective tool. However, such datasets are not sufficiently available to the community.

Throwing sand in the gears

A third important task is dealing with anti-forensics, i.e., all measures taken by attackers to cover up or destroy their tracks. Anti-forensics have always been used by criminals. For example, a burglars wear gloves to avoid leaving telltale fingerprints. In digital forensics, it is important to understand and detect anti-forensic methods used by attackers.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

One challenge of IT forensics is to secure and analyze data.

FIG.: ADOBE STOCK / NOPPONPAT; MICROGEN

Investigation of DIY Drones

IT forensic data analysis: DIY drones in the focus of law enforcement

In addition to commercial drones, the dynamically growing market for unmanned aerial systems also offers a wide range of kits that can be used to build so-called DIY drones. Drones are also increasingly being used for criminal activities, such as preparing and carrying out drug smuggling or theft offenses, and can be customized to meet specific needs.

DRONES can be divided into different categories according to characteristics such as the size, weight, span, intended use or even regional legislation.

Prosecution

The number of drones used in investigations in connection with the IT forensic preservation and examination of digital evidence is constantly increasing.

To date, the majority of drones seized have been commercial drones, which are usually processed using standard commercial software for securing and analysis.

DIY drones

However, manufacturers of forensic software do not pay attention to the area of do-it-yourself drones. These flight systems are individual parts or kits that can be customized. Drones can be highly customized in terms of functionality and performance or can be less expensive if lost. DIY drones can be used in cases such as to circumvent no-fly zones or spy on properties.

These customization options mean that commercial software packages often cannot be used to secure and investigate DIY drones, because they do not offer the option of backing up or analyzing the new interfaces and data formats.

DIY drone of the Digital Forensics research group, which is used in the FOCUS project together with other reference devices for data generation.

Digital forensics

The data generated on the seized drones can be helpful in solving criminal offences.

During the use of a drone, data such as flight altitude, speed, take-off and return locations, defined flight routes or even recorded image and video material can be secured.

Digital forensics methods can be used to track down and read out the data memories of drones. This can provide law enforcement authorities with important investigative leads.

FOCUS project

The Forensic Examination of DIY Drones (FOCUS) addresses the investigation of two scenarios:

1. Discovery of a drone in connection with criminal activities and
2. Loss of a drone during use by security authorities.

The research focuses on extracting and analyzing stored data. Scenario One is aimed at securing evidence. Scenario Two attempts to prevent unauthorized access to the data.

The aim of the project is to develop recommendations for the use of DIY drones and tool chains for forensic investigations that can be used for criminal prosecution.

HptFw d. R. Mario Winkler, M.Sc.

mario.winkler@unibw.de

+49 89 6004 7346

www.unibw.de/digfor

Funded by: German Federal Ministry of Education and Research (BMBF)

FIG.: RI CODE / MARIO WINKLER

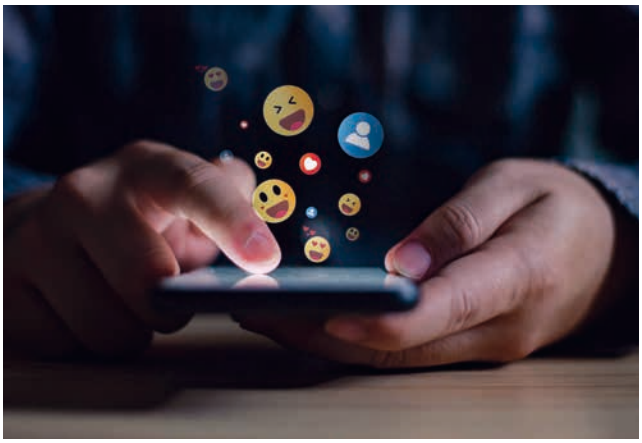
To possess or not to possess ...

... that is the question: Illegal WhatsApp stickers on Android and their prosecution

WhatsApp stickers are a popular mix of emoticons and user-created images or videos. They are not subject to any authoritative control but are automatically shared from peer to peer in chats. As a result, they can go viral—not just the funny ones, but also the illegal ones. This puts users in the unfortunate position of having incriminating media files on their device without knowing or wanting to, and law enforcement in the unexpectedly difficult position of distinguishing perpetrator from victim.

From funny to illegal

Meta introduced stickers to WhatsApp in 2018, and since then, the ease of creating them has gradually increased. At the moment, Meta makes it possible for all users to create their own stickers from any image in an instant. This seems like good news. After all, stickers are mostly shared for legitimate purposes. However, users also share stickers with illegal content, such as Child Sexual Abuse Material (CSAM) or Nazi propaganda. On the one hand, law enforcement and the courts have been confronted with cases where users have unknowingly received CSAM in ordinary group chats. On the other hand, there are cases where users have engaged in the very activities that the law is designed to punish.



The prosecution of illegal WhatsApp stickers is a challenging task.

Prosecutable possession?

These cases usually revolve around the question of whether the user is in possession of such an illegal sticker. Interestingly, the concept of possession is easy to translate to the digital world, but hard to decide. In most jurisdictions, possession means that a person has actual control over an object, in this case a sticker, and that the person knows of its existence. Some laws also require intent as a condition of possession. However, this means that it is possible to use technical ignorance as an argument against having actual control or knowledge of a file. Obviously, it is not the intent of the law that intentional interactions with CSAM go unpunished for allegedly technically unsophisticated individuals.

Results enable prosecution

To provide valuable insights for law enforcement and digital forensics practitioners, the Professorship of Digital Forensics conducted a thorough digital forensic analysis of the entire lifecycle of community-created stickers. Most importantly, the results clearly show that simply finding a sticker on an Android device is not sufficient to infer possession, as a sticker can be acquired without knowledge of its existence. Furthermore, the research provides a detailed guideline for law enforcement to convict an offender of distributing or possessing illegal stickers.

This research will hopefully contribute to ongoing efforts to combat the distribution of illegal content through messaging apps, while also helping innocent people caught in the middle.

Samantha Klier, M.Sc.

samantha.klier@unibw.de

+49 89 6004 7346

www.unibw.de/digfor

FIG.: ISTOCK / CHOOCHART CHOOCHAIKUPT

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

The research group headed by Stefan Brunthaler focuses on language-based security, an area that investigates the use and applicability of language-based transformations to secure vast amounts of software in a way that is automated, transparent, and effective. A key aspect of these techniques is that they offer unparalleled scalability, as evidenced by the ability to compiler hugely complicated software such as web browsers.

THE Munich Computer Systems Research Laboratory (µCSRL) continued on its Clausewitz-inspired journey "language-based security is the continuation of compiler construction by other means."

In 2024, we maintained our steady growth trajectory by having two Master's students from TU Munich conducting their thesis research in our lab, Matheo Vergnolle and Alina Weber-Hohengrund. Matheo Vergnolle did a double degree from Ecole Polytechnique and went back to Paris after finishing his outstanding Master's research project, namely the extension of our Dependable Production Systems (DEPS) research project into the data domain, i.e., instead of triggering bit flips in code, Matheo examined the capability and utility of flipping bits in data. Alina investigated a novel direction of diversification to achieve lightweight compartmentalization in the node.js ecosystem and used Oracle Lab's Graal ecosystem to do so. Finally, we welcomed a new PhD student to µCSRL: Tim Matussek from HHU Düsseldorf joined the lab in September.

As planned, we were able to publish several papers in highly competitive and reputable venues, such as the 38th European Conference on Object Oriented Programming (ECOOP), the 21st Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), and the 3rd Fuzzing Workshop, co-located with the International Symposium on Software Testing and Analysis (ISSTA) in Vienna.

The entire research group attended the 40th Workshop of the GI special interest group on programming languages and computational principles in Bad Honnef. Prof. Brunthaler also attended the IFIP Working Group 2.4, Software Implementation Technology, meeting in Lugano, Switzerland, and the DWT meeting on "Software-Defined Defense" in Bonn.

From a research perspective, 2024 proved to be enormously fruitful, with new results in optimizing Python (see the ECOOP'24 Cross-Module Quickening paper documenting up to 3x speedups for Python programs using NumPy), as well as important progress made on our fuzzing endeavors, such as the completion of a warehouse-scale heterogeneous fuzzing infrastructure, which also supports a novel combinatorial-optimization technique. As a result, we expect numerous publications in 2025 and onwards. For our undergraduate lectures in systems programming and our graduate compilers course, we developed a new approach that includes new interactive lecture notes based on Jupyter Books.

Prof. Dr. Brunthaler served on the 2024 ACM SIGPLAN International Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA'24 in Pasadena, CA, USA), with revisions reviewed for the 2025 installment, the IEEE SecDev conference and, finally, continued to serve as the Area Chair for System Security for the *Journal of Systems Research* (*JSys*).

The µCSRL research group received funding from the German Ministry of Defense, and the Austrian Research Promotion Agency.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

https://unibw.de/ucsrl

FIG.: ISTOCK / DE M10

Cross-Module Quickening—The Curious Case of C Extensions

Breaking down the optimization barrier posed by separate compilation units, such as NumPy or PyTorch.

Python offers high productivity and a large library ecosystem, but there are applications where the proverbial need for speed is lacking. To accommodate such scenarios, Python offers an escape hatch through C extensions, as do many other similar languages as well. These C extensions extend Python either through providing abstractions Python does not yet offer, or by speeding up Python code that becomes a bottleneck.

LET'S ILLUSTRATE C extensions using NumPy as an example. Python itself lacks a datatype for multi-dimensional arrays that are co-located in memory. Instead, Python's native arrays are jagged, with each dimension stored in non-adjacent memory locations. This structure prevents the use of efficient data-parallel instructions (SIMD), making heavy numerical computations painfully slow. The NumPy extension adds a datatype offering memory co-location to Python, which enables the use of high-performance SIMD instructions.

C extension speedups are separate from Python optimizations, which led to systems like Numba and NumPyPy. Numba compiles Python code to machine code, but requires manual source code changes and imposes limitations on Python's dynamic behavior. Meanwhile, NumPyPy constitutes a rewrite of NumPy's C code in Python, allowing PyPy's JIT compiler to optimize it. Both approaches face challenges: Numba requires constant updates for new Python versions, while NumPyPy must adapt whenever NumPy changes.

In 2024, µCSRL members Felix Berlakovich and Stefan Brunthaler introduced Cross-Module Quickening (CMQ). CMQ builds on Brunthaler's earlier research that has been officially adopted since Python version 3.9. The core idea is that an interpreter can mimic JIT compilers by continuously replacing slower interpreter instructions with faster ones. This technique could not, however, optimize across separate compilation units. Since one cannot tell their interior layout after compilation, these units are black boxes. CMQ lifts the lid of these boxes by providing an optimization interface that allows extensions to expose internal data. The interpreter, in turn, adapts dynamically to leverage these internal data, addressing a longstanding challenge in optimizing across compiled units.

To evaluate the idea, both Felix and Stefan set to work on an implementation prototype, which took about four months to finish, primarily due to unfamiliarity with the NumPy internals. Benchmarking against NPBench from ETH Zurich revealed significant optimization opportunities. CMQ achieved speedups of up to 3x in certain scenarios. However, in cases where numerical computing dominates CPU time, the interpreter's overhead is negligible, offering no significant speedups.

In summary, CMQ represents a significant step forward in bridging the optimization gap between Python and its C extensions. By enabling optimizations across module boundaries, it provides a flexible and efficient alternative to existing approaches, making Python faster and more capable for numerical and scientific computing, both of which are at the core of many machine learning applications.

Felix Berlakovich
felix.berlakovich@unibw.de
+49 89 6004 7332
www.unibw.de/ucsrl

LOOL: Low-Overhead Optimization-Log-Guided Compiler Fuzzing

Increasing compiler fuzzing efficiency through using optimization logs.

LOOL: Low-Overhead Optimization-Log-Guided Compiler Fuzzing introduces a novel approach to testing compilers by tapping optimization logs—detailed records of code transformations—as a lightweight alternative to code coverage. Implemented in GraalVM, LOOL uses genetic algorithms to focus on untested paths, uncovering bugs more efficiently.

COMPILERS ARE essential tools that translate code written by developers into machine-readable instructions. Bugs in compilers can, however, lead to incorrect program behavior, crashes, or security vulnerabilities, which are notoriously difficult to detect. To identify such bugs, developers often rely on fuzzing, a technique that generates large amounts of test code and subsequently executes generated test code to explore the resulting compiler. Traditionally, fuzzing tools use code coverage as their primary feedback mechanism, which measures how much of the compiler's internal logic is "touched upon" by the test cases. While effective, this approach has significant downsides: it can be resource-intensive and often misses less-tested or complex regions of the compiler.

In 2024, µCSRL member Felix Berlakovich and colleagues from Oracle Labs Austria and the University of Linz, Austria, proposed a new method, Low-Overhead Optimization-Log-Guided Compiler Fuzzing (LOOL), which offers an alternative approach to fuzzing. LOOL leverages a key feature of modern compilers: optimization logs. These logs, generated during the compilation process, document the transformations a compiler applies to code, such as removing redundancies or improving performance. LOOL uses these logs as a low-cost and detailed source of feedback, helping the fuzzing tool to focus on areas of the compiler that might otherwise be overlooked. This technique reduces overhead while maintaining—if not improving—the quality of bug detection.

To evaluate the practicality and utility of compilation-log driven fuzzing, LOOL was implemented in the GraalVM fuzzing framework. To effectively guide the fuzzing process, a genetic algorithm was used, which mimics natural selection to evolve test cases over time. By analyzing optimization logs, the algorithm can prioritize generating inputs that exposed untested paths in the compiler. This approach was particularly valuable for targeting areas of the compiler that interact with complex optimizations, which are often difficult to test using traditional methods.

Developing the LOOL prototype took several months, partly due to the intricacies of integrating it into the GraalVM framework. Once completed, the LOOL prototype evaluation demonstrated significant improvements in bug detection on real-world benchmarks. In some cases, LOOL uncovered previously unknown issues that traditional code coverage-based fuzzing failed to find. The low overhead of optimization logs, furthermore, made the process more efficient, enabling broader and deeper exploration of the compiler's logic.

LOOL represents a promising advancement in compiler fuzzing. By harnessing information already generated by compilers, LOOL enables faster, smarter, and more cost-effective testing. While it does not eliminate the need for traditional fuzzing tools, it complements them by addressing gaps in their capabilities and expanding the range of detectable bugs. This new method lays the groundwork for further innovations in testing and debugging tools for modern compilers in general, and just-in-time compilers in particular.

Felix Berlakovich
felix.berlakovich@unibw.de
+49 89 6004 7332
www.unibw.de/ucsrl

Prof. Dr. Michaela Geierhos

Data Science

The interdisciplinary team of the Professorship of Data Science combines expertise from the fields of computer science and computational linguistics to address current and future-oriented research questions in the areas of semantic information processing and knowledge & data engineering.

Applied research

Data Science is an applied, interdisciplinary science. Its aim is to generate knowledge from data, for example in order to support decision-making processes. It uses methods and insights from fields such as statistics, stochastics, computer science, and computational linguistics.

The Professorship of Data Science researches methods for extracting information from data and develops data-driven solutions by processing, preparing, analyzing, and inferring large amounts of data (Big Data). In particular, this includes the development of algorithms for (semantic) text analysis, which has practical applications in social media mining that, in turn, can be used to detect threats to objects of protection or to identify disinformation campaigns. The type of data is very diverse: In addition to text, audio signals and images are also processed.

Practice-oriented training

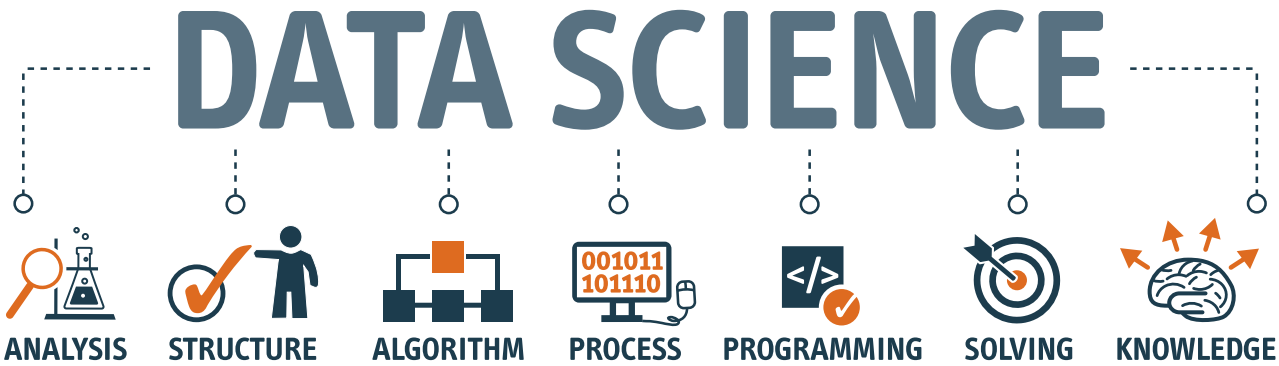
All Data Science courses are based on a teaching concept that combines theory and practice. Right from the start, students benefit from the opportunity to directly apply the theoretical knowledge acquired in the lectures in a variety of exercises and diverse practical projects. In this way, the Professorship of Data Science contributes to the excellent academic education of students at the University of the Bundeswehr Munich.

Data science use cases: Practice-oriented research

The Data Science team maintains numerous collaborations with partners from the military, industry and the public sector in order to combine theory and practice in research. The areas of application currently range from the detection of disinformation campaigns and the identification of deepfakes to the use of trustworthy AI in police applications. One research objective deals with the constant threat of cyberattacks. Information-rich Cyber Threat Intelligence reports provide in-depth insights into the tactics, techniques and procedures of attackers as well as the latest threats and vulnerabilities. The goal is to extract structured knowledge from these reports, which will be transformed into a graph that enables temporal analysis and prediction of correlations based on existing knowledge in the field of cyber security.

Another research objective is to develop an early warning system for the vulnerability of objects of protection by analyzing activity data in running apps and user-generated data in other social networks. Users often have accounts on several social networks where they disclose different personal information. By combining all available information, users can be clearly identified, which increases the risk of identity theft or social engineering. A particular danger arises when users publicly share their geo-data from running apps. This data can be used to create physical movement profiles and localize military locations, for example. By comparing such data with other confidential data (e.g., from military agencies), it is possible to determine the plausibility of a threat to individuals.

Prof. Dr. Michaela Geierhos
michaela.geierhos@unibw.de
+49 89 6004 7340
www.unibw.de/datascience



Range of tasks covered by the Professorship of Data Science.

FIG.: ADOBE STOCK / AI FARM; SHUTTERSTOCK / TRUEFFELPIX

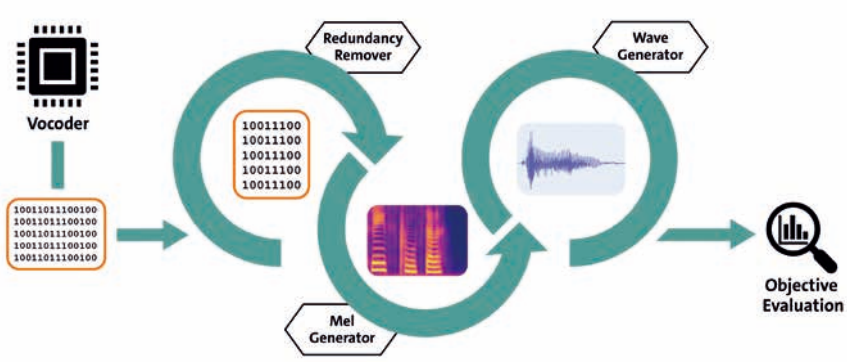
Project AI-based Audio Decoder

Neural networks for speech signal decoding

Proprietary vocoders are typically used for the transmission of audio data. These consist of two components: an encoder that converts the audio data into a bitstream before transmission on the sender side and a decoder that interprets the bitstream back into an audio signal on the receiver side. This project deals with the question of whether neural networks can replace the decoder.

Architecture of the AI-based decoder

The task of the AI-based decoder is to decode an encoded bitstream and reconstruct the speech information. The reconstruction of the bitstreams is achieved through three consecutive neural networks. In the first step, a network is used to remove redundancy. The subsequent network, the Mel Generator, transforms redundancy-free bitstreams into Mel spectrograms. Finally, the Wave Generator network produces playable audio files in the wave format. To automatically evaluate the quality of the generated audio files, two methodologies are employed.



Overview of the architecture of the three consecutive neural networks to generate an AI-based decoder.

Redundancy remover

Redundancy refers to information that is transmitted in addition to the actual data. This information can be used by the receiver to correct any errors that occur during data transmission. The following networks work on the basis of redundancy-free bit streams, which is why this network is used.

Mel Generator

Using the Mel Generator, so-called Mel spectrograms are generated from the redundancy-free bitstreams. These represent the audio information in a discrete form. The spectrograms are based on the Mel scale, which mimics human sound perception. To keep the bandwidth low, the vocoders under consideration operate at a low sampling rate. This rate can be increased by the Mel Generator so that CD quality is achieved.

Wave Generator

Generating playable wave files from Mel spectrograms is a common component of text-to-speech systems, so promising frameworks (e.g., MelGAN or HifiGAN) already exist in this area of research and are used here.

Evaluation

To objectively evaluate the resulting audio files and thus the speech reconstruction, two methods are employed:

1. **Based on Transcription:** A neural network transcribes the audio data and the transcription result is compared with the original transcript of the audio dataset.
2. **Based on Audio Evaluation Algorithms:** To evaluate communication channels, algorithms have been developed that compare two audio signals with each other. The comparison result is usually a score between 1 (“unintelligible”) and 5 (“no quality loss”) on the Mean Opinion Scale.

Hendrik Bothe, M.Sc.
hendrik.bothe@unibw.de
+49 98 6004 7343
https://go.unibw.de/vocoder

FIG.: RI CODE / H. BOTHE

Project KiTIE

Identification and evaluation of cooperation partners based on patent information

Technology transfer, particularly in large research institutions, is often constrained by complex partner search processes. Given increasingly interconnected innovation processes, the KiTIE project is developing an intelligent platform that systematically identifies potential partners for research institutions through the analysis of patent, publication, and company data.

How does the intelligent partner matching work?

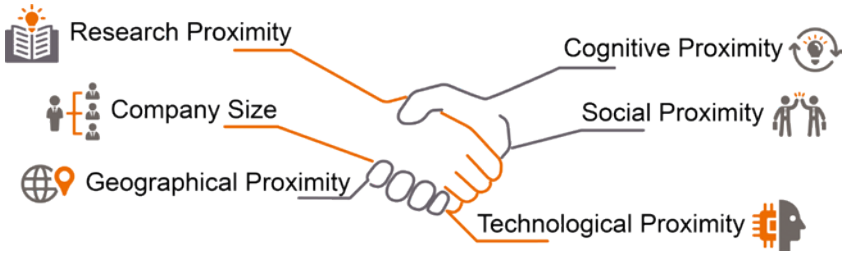
The platform processes data such as patents, scientific publications, research projects, website texts, and company information using semantic analysis and AI methods. The matching process begins with the entry of a technology description and involves the following steps:

1. **Patent Class Classification:** Classification of technology descriptions into patent classes using a combination of semantic search and Large Language Models (LLMs).
2. **Company Profiling:** Analysis and classification of company data to create technological company profiles based on patent classes.
3. **Matching Analysis:** Comparison of technology description and company profile with regard to technological proximity and technological complementarity.

Why is intelligent matching relevant?

Traditional partner search in technology transfer often relies on personal networks, reaching its limits with increasingly complex technological challenges. Data-driven evaluation of potential partners based on various data sources and indicators becomes key for successful technology transfer. In the KiTIE project, a multidimensional evaluation system analyzes the suitability of potential partners based on defined proximity indicators:

- **Research Proximity:** Alignment of scientific focus areas
- **Technological Proximity:** Compatibility of patent portfolios
- **Cognitive Proximity:** Similarity in innovation processes
- **Social Proximity:** Existing cooperation relationships
- **Structural Proximity:** Geographic and organizational compatibility



The KiTIE platform considers various indicators between organizations to identify optimal cooperation partners.

Development of the interactive KiTIE platform

The platform enables researchers to identify suitable cooperation partners based on their project description. A matching score is calculated for the search results, which quantifies the suitability of the candidates. The interactive user interface offers flexible filter options and presents the matching results in a transparent manner. The processed company profiles with relevant key figures and information enable well-founded decision-making. The analysis results can be explored in interactive network visualizations and enable detailed partner comparisons. A prototype is currently undergoing a systematic development and evaluation process. The design is therefore user-oriented with the integration of pilot application feedback, and the platform functionalities are implemented iteratively. In addition, continuous adaptation to real usage scenarios is taking place.

Benjamin Vehmeyer, M.Sc.
benjamin.vehmeyer@unibw.de
+49 89 6004 7341
https://go.unibw.de/kitie

Funded by: German Federal Ministry of Education and Research (BMBF)

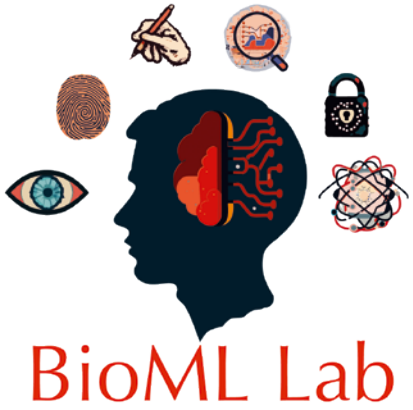
FIG.: RI CODE / B. VEHMEYER

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

The BioML Lab, led by Prof. Dr. Marta Gomez-Barrero, holder of the Professorship of Machine Learning, researches methods to develop reliable, secure, fair and privacy-friendly biometric recognition systems. The focus of the group is on highly innovative and applied IT-security interdisciplinary research, building upon machine and deep learning architectures as well as cryptographic methods.

BioML: Biometrics and Machine Learning Lab



BioML: Biometrics and Machine Learning research group.

The BioML Lab was established in October 2023 and is part of the Research Institute CODE and the Department of Computer Science. Led by Prof. Dr. Marta Gomez-Barrero, holder of the Professorship of Machine Learning, BioML researches methods to develop reliable, secure, fair, and privacy-friendly biometric recognition systems. The focus of the group is on highly innovative and applied IT-security interdisciplinary research, building upon machine and deep learning architectures as well as cryptographic methods.

BioML co-organizes and participates in international academic conferences such as the IEEE Int. Joint Conference on Biometrics (IJCB) and the IEEE Int. BIOSIG Conference and contributes both to the European Association for Biometrics (EAB) and the international standardization in ISO/IEC JTC1 SC37.

Research foci at BioML Lab

Biometric recognition refers to the automated recognition of individuals based on their behavioral and biological characteristics. Examples of such characteristics within the scope of the group include face, iris, fingerprint, finger vein, or handwritten signatures, as well as combinations of those in multi-biometric schemes. Besides trying to increase the recognition accuracy and computational efficiency of the systems, the lab focuses on other relevant aspects of this research area. Preserving the privacy of the subjects is at the core of the research, for which the lab develops biometric template protection schemes in compliance with the European General Data Protection Regulation (GDPR) and relevant ISO standards, following the Privacy-by-Design principle. Furthermore, the detection of several forms of attacks on biometric systems (e.g., presentation attacks or morphing attacks) is key to increasing the security and reliability of the systems. Last but not least, the team aims at the explainability and transparency of the algorithms to allow further acceptance and deployment of biometric recognition.

Activities

2024 was a busy and eventful year at BioML Lab. Three graduate researchers joined the group: Erik Trolliet, Osman Demir, and Camilo Linares. They started researching several topics: biometric template protection systems based on deep hashes for iris and fingerprint samples; presentation attack detection methods for iris and facial images; the benefits of large language models for biometric recognition; and the use of synthetic data to enhance biometric systems.

On an international level, we have reinforced our collaborations through different activities. We are editing the upcoming Springer “Handbook on Biometric Template Protection”, together with Vedrana Krivokuca and Sébastien Marcel from Idiap (Switzerland) and Arun Ross from Michigan State University (USA). Marta Gomez-Barrero is also leading the review process of the ISO/IEC standard 30136 on “Performance testing of biometric template protection schemes”, which has reached a CD stage in the last ISO SC 37 meeting in Wellington. Through the European Association for Biometrics (EAB), we co-organized the Martigny Biometrics Workshop with the US Center for Identification Technology Research (CITeR) and the Idiap Research Institute. In addition, we once again co-organized the Darmstadt Biometrics Week together with the Fraunhofer IGD. We have also started new initiatives, such as the EAB Council of Wisdom, where experts answer questions from the public on different topics related to biometric recognition.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

FIG.: ADOBE STOCK / DILOK; FI CODE / MARTA GOMEZ-BARRERO

Synthetic Data and Biometrics

Advantages and challenges of using synthetic data in biometric recognition systems

Synthetic facial images can be used for the creation of deepfakes, most likely with bad intentions, but can also serve good purposes. For instance, if we were able to generate images for underrepresented minorities in our training data, we could tackle bias against those groups. Despite the multiple approaches to synthetic image generation, its utility for biometric recognition is not yet clear.

Synthetic data for biometrics

There is a number of reasons for using synthetic data in biometric recognition systems. First of all, collecting the large datasets needed to properly train deep learning algorithms is not always feasible. Thus, by using synthetic data, we could increase the size of our datasets. Moreover, we can also focus on underrepresented groups (e.g., the elderly in the data collection at a university, or ethnic groups less present in a given area), so that the biometric system learns how to properly recognize them. From another perspective, if we used synthetic instead of real data, we could decrease the privacy risks derived from a data breach.

Synthetic faces can improve the training of biometric recognition systems.

FIG.: ADOBE STOCK / STUDIO F.

Biometric quality and diversity

Despite the high number of publications on the generation of synthetic facial images, there are still some challenges for their use for biometric purposes. First and foremost, even if those synthetic images are visually realistic, they don't always present high biometric quality. This refers not only to the sharpness of the image, but also to other properties that can eventually lead to a poor recognition performance: an extreme facial expression or poor illumination. Similarly, many models suffer from a low diversity, as only a handful of identities can be synthesised. However, for large-scale biometric applications, we require correspondingly large number of identities to be able to capture the variability present in real subjects.

Benchmark

Taking into account the aforementioned challenges, we are benchmarking several models based on Generative Adversarial Networks (GANs) or diffusion models in terms of biometric quality and diversity. To that end, we use both traditional quality metrics such as BRISQUE and the Open Source Face Image Quality (OFIQ) from the German BSI, soon to be included in the ISO/IEC 19794-5 as the standard implementation of face image quality metrics. We also estimate how many identities can be generated from the different models. The next steps will focus on the best models to generate a large synthetic dataset that we will use to enhance several aspects of biometric recognition systems.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

Biometrics and Privacy

How to extract deep hashes from iris images

A common approach to protect passwords both for storage and transfer uses cryptographic hashes. When we talk about biometric data, such as iris images, we cannot employ common hash algorithms like the SHA or the MD families due to the noisy nature of biometric data: A single bit flip leads to completely different hashes. We thus need to investigate other ways of extracting hashes from iris images.

What is biometric template protection?

Biometric data has been classified as sensitive personal data by the European General Data Protection Regulation (GDPR). Thus, in order to deploy and use biometric systems, we need to protect the data end-to-end: for storage, transfer, and any kind of processing. The ISO/IEC 24745 standard defines the properties that so-called biometric template protection (BTP) schemes need to fulfill, and the ISO/IEC 30136 gives guidelines on how to test these schemes with regard to privacy protection.

To protect people's privacy, deep hashes can be extracted from iris images.

Deep hashes

Among the different BTP methods developed in the last two decades, there is a new trend using deep learning algorithms not only to carry out biometric recognition, but to simultaneously protect the underlying data. In particular, we have focused on the use of maximum entropy binary (MEB) codes, which have already been extracted from facial images. This approach has three stages: 1) First, we use a convolutional neural network (CNN) to generate templates with a reduced intra-class variability (e.g., two facial images from the same person lead to very similar templates); 2) we then combine those templates with pre-defined MEB codes; and 3) we apply common cryptographic hashes to those codes to generate the final protected templates (similar to text based password protection). Such a methodology has several advantages: The cryptographic hash function is non-invertible, and it should be very difficult to recover an MEB code from its hash; even if MEB code is recovered, it does not reveal the face template to which it was assigned; and we can assign new MEB codes in the event of compromise (remember we can change a password, but not our face or iris!). The main challenge remains in the generation of those templates exhibiting a low intra-class variation.

Iris deep hashes

Iris images show less variance between acquisitions than facial pictures. We have therefore focused so far on this biometric characteristic. With a lightweight CNN, we generated 256-bit MEB codes and then applied SHA-512. In a database with 100 subjects, we achieved a promising False Match Rate of 7%. This is of course higher than the error rates achieved with unprotected data. We will continue working on decreasing these errors and also analyze further privacy protection properties such as the unlinkability of templates enrolled in different applications.

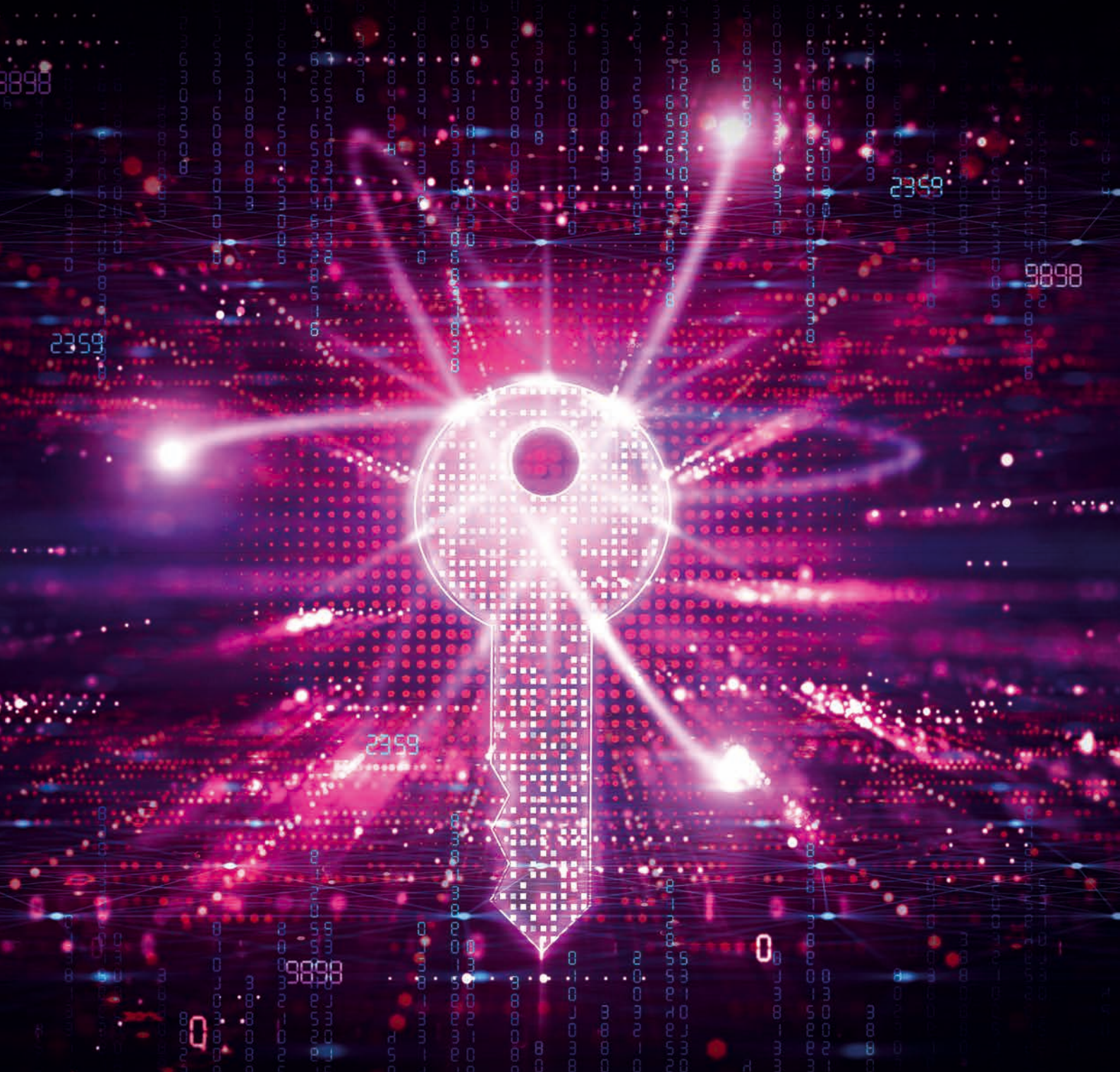
Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

FIG.: ADOBE STOCK / TANYA



Prof. Dr. Udo Helmbrecht

Quantum Communication

Within the framework of dtec.bw, the MuQuaNet project is constructing a quantum network in the Munich metropolitan area in cooperation with partners in academia and industry. The goal is to establish test and research operations of a quantum communication network with selected civil and military applications.

MuQuaNet: Pioneering work for quantum-secure communication in the greater Munich area

Within the framework of the research project MuQuaNet (Munich Quantum Network), a quantum network is being established in the greater Munich area in collaboration with academic and industrial partners. Supported by dtec.bw, this initiative aims to develop a forward-looking communication infrastructure based on quantum mechanical phenomena and the use of quantum objects to meet the highest security standards. The deployment of Quantum Key Distribution (QKD) will explore and test the secure transmission of data for both civilian and military applications.

Goals and approach

The primary goal of MuQuaNet is the establishment, evaluation, and operational testing of a quantum network that meets modern security requirements and offers innovative approaches to data transmission. A focus is on testing the practical applicability of QKD in real scenarios, especially in security-critical areas such as defense. The infrastructure connects various sites, including the campus of the University of the German Armed Forces (UniBw), as well as partner institutions like the German Aerospace Center (DLR), Ludwig Maximilian University (LMU), Airbus, and other partners from industry and academia.

Key management as a core aspect

A central element of the project is key management, which forms the basis for security in QKD systems. Challenges such as the lack of standards and the reliability of intermediate nodes are addressed through innovative approaches like the Multi-Path Key Reinforcement (MKR) developed in the project. This method distributes key material across multiple paths to increase robustness and security in complex networks.

Application example: VR remote maintenance of a frigate

A prominent use case of the project is the remote maintenance of frigates using virtual reality (VR) via satellite links. Here, QKD is used to meet the high security requirements of these sensitive communication scenarios. MuQuaNet developed a special free-space QKD system in collaboration with LMU and investigated its integration into satellite communication with the DLR. These efforts highlight the importance of QKD for security-critical military applications.

3D-printed frigate model with sensors for QKD-encrypted remote maintenance via VR glasses.

Perspectives and benefits

MuQuaNet makes a significant contribution to the development of secure quantum communication systems and supports the German Armed Forces and other authorities in protecting sensitive data. The insights and technologies gained from the project will not only advance scientific progress but also strengthen industrial innovation. In the future, the network will be expanded to include additional sites, applications, and partners to optimize the practicality of QKD in various scenarios and strengthen Europe's leading position in the field of quantum-secure communication.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 2495

www.unibw.de/muquanet

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.

dtec.bw

Funded by the European Union
NextGenerationEU

FIG.: SHUTTERSTOCK / ARTEMISDIANA; FI CODE / S. KASTRUP

3-km Free-Space QKD Testbed

A self-developed decoy-state sender enables robust QKD in realistic atmospheric conditions

MuQuaNet's 3-km free-space quantum link between ETTI and Airbus demonstrates robust QKD in realistic outdoor conditions. A decoy-state BB84 sender, jointly developed by LMU and UniBw, operates at 850 nm with minimal SWaP (size, weight, and power)—a key requirement for mobile QKD. The ground link approximates atmospheric effects of a LEO (Low Earth Orbit) satellite-to-ground scenario, although geometric losses over longer distances remain significantly higher.

ONE STEP TOWARD practical quantum communication is the 3-km free-space QKD link established between the University of the Bundeswehr Munich (UniBw M) and Airbus. At the core of this custom-built demonstrator is a compact, low-power decoy-state BB84 sender operating at 850 nm. The transmitter's minimal size, weight, and power (SWaP) profile addresses key real-world constraints, from ground-based outdoor deployments to potential future scenarios that may demand tight packaging. The system runs at a 100 MHz modulation rate and relies on an FPGA for both signal generation and fine-tuned adjustments to quantum protocol parameters.

Preliminary measurements conducted in daylight conditions around 5 p.m. show secret key rates of roughly 500 bit/s, with considerable potential for improvement through further optimization of optical components, alignment protocols, and protocol parameters. Fast steering mirrors will actively compensate for beam drift caused by turbulence, vibrations, and temperature gradients, while employing the 1550-nm beacon—now used solely for synchronization—for classical communication promises standalone operation. Ongoing refinements target higher stability, minimized error rates, and improved maintainability, which are pivotal for real-world adoption.

Exposing the link to open-air conditions allows to observe how humidity, light pollution, and temperature shifts affect QKD outside well-controlled laboratories. Small environmental fluctuations can degrade alignment or alter background noise, prompting adjustments in beam pointing and protocol settings. By documenting these factors alongside performance logs, we can refine both hardware and control algorithms to harden system resilience over longer operating periods.

Though the link primarily functions as a short-distance demonstrator, it also supports broader goals within MuQuaNet by informing how free-space QKD might integrate into larger networks. Data gathered here helps outline strategies for scaling QKD to more extensive deployments, as the dense atmospheric layer over 3 km approximates atmospheric effects of a 500-km Low Earth Orbit (LEO) satellite-to-ground downlink.

This free-space QKD link serves as an important testbed for ongoing efforts to integrate quantum security into real-world communication infrastructures. In the future, the insights gathered are expected to help developments in satellite QKD, where adjusting for atmospheric effects will be essential in achieving robust global quantum cryptographic coverage.

Michael Auer

michael.auer@unibw.de

+49 89 6004 7374

https://go.unibw.de/eq

Funded by: Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.

dtec.bw

Funded by the European Union
NextGenerationEU

Security Analyses of QKD Systems

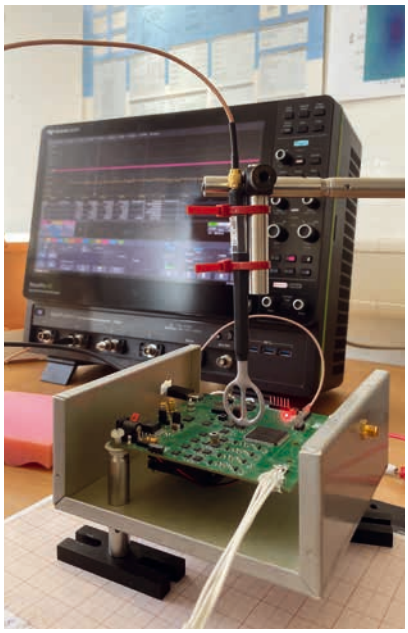
During the reporting period, the focus of the work was on evaluating security risks and developing countermeasures against attacks on QKD systems. The analyses are divisible into three areas: quantum hacking, classical IT attack vectors, and analysis of electromagnetic emissions.

Quantum hacking

Quantum hacking refers to attacks on quantum optical components to manipulate key material or restrict the key space. This is based on the BSI report "Implementation Attacks against QKD Systems" published in 2023, which systematically summarized and categorized a large number of quantum optical attack vectors from scientific publications. Together with a manufacturer, the "Detector Efficiency Mismatch" attack was performed on a commercially available QKD system. During this attack, some of the detectors necessary for the technology were deliberately switched off or restricted in efficiency to influence the key space. The resulting key material was then analyzed using statistical methods. We were able to demonstrate that the manufacturer's proprietary countermeasure effectively mitigated this attack.

Classical IT attack vectors

In this project part, classical penetration tests were performed on the IT components of the QKD devices. After initial reconnaissance, an initial access point was identified using various scanning methods. Privilege escalation techniques allowed obtaining administrative rights on the device to establish persistence. Moreover, data exfiltration would have been possible. Found vulnerabilities were reported to the manufacturers through a responsible disclosure procedure, including assistance for remediation. The project thus contributes to strengthening the IT security of German QKD solutions.



Measurement of electromagnetic emissions from a QKD component.

FIG.: MUQUANET / M. KAACK

Analysis of electromagnetic emission

QKD devices can produce electromagnetic emissions, which can be measured with special equipment. The collected data can be correlated and potentially allow conclusions to be drawn about the generated key material. In an initial experiment, raw key material could be extracted. Further experiments and concepts for protection against this type of attack are currently being planned.

David Koch

david.koch@unibw.de

+49 89 6004 7328

https://go.unibw.de/em

Funded by: Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.

dtec.bw

Funded by the European Union
NextGenerationEU

Prof. Dr. Wolfgang Hommel

Software and Data Security

Wolfgang Hommel's team researches technical and organizational security measures for complex IT infrastructures and communication networks with an increased need for protection as well as their practical application under the motto "Development and operation of secure networked applications."

THE TEAM OF the Professorship of Software and Data Security pursues the goal of developing solutions for real-world-relevant security challenges under the consideration of operational boundary conditions, that are typically part of the operation of complex IT infrastructures.

Research and projects with third parties therefore usually begin with a comprehensive empirical analysis, in which, for example, relevant components from the designated application area are cloned into virtual environments or at least their core characteristics are modeled and simulated to facilitate detailed analysis. This approach allows, among other things, the explorative application of offensive test procedures and thus the qualitative and quantitative analysis of vulnerabilities in complex multi-step attack scenarios. From this, security requirements can be systematically derived, which serve as a basis for the subsequent constructive activities and a later practical evaluation of the results achieved.

The design of new and improved IT security measures follows the security engineering approach: On the one hand, they are designed, modeled, and simulated on a technical level. On the other hand, they are integrated as seamlessly as possible into the design, implementation, and operational processes of the intended application areas, also from an organizational perspective. An essential requirement is the concrete implementation with subsequent evaluation, which takes place at a minimum in the laboratory, but if possible, also in concrete pilot environments, and ideally by individual embedding in scientifically accompanied projects. The role of the human factor in information security, economic and legal constraints is also taken into account.

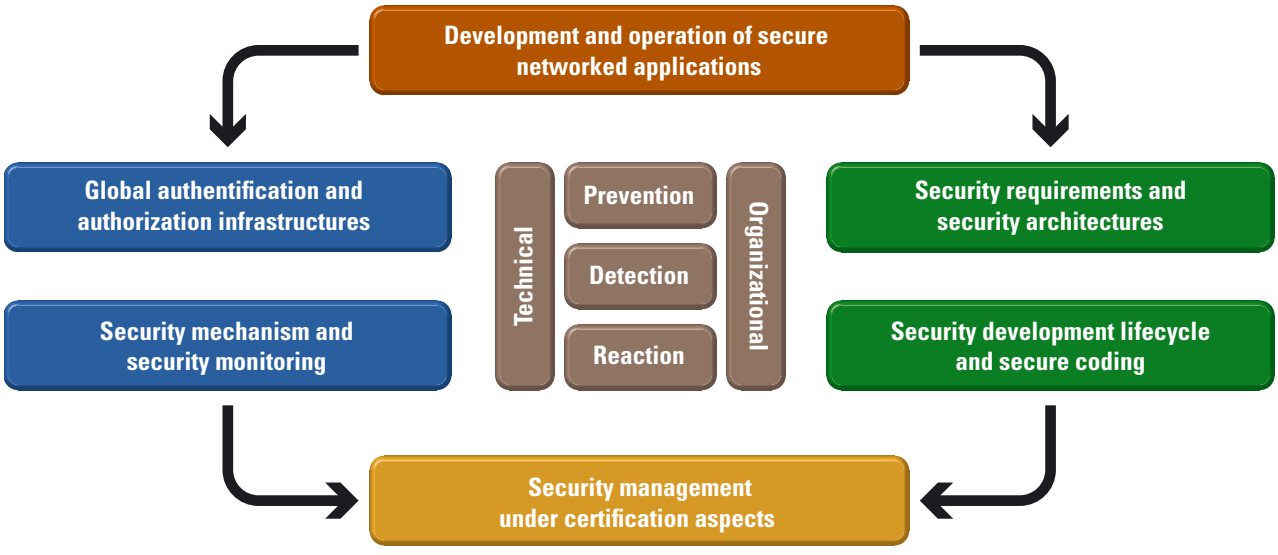
In ongoing research projects and projects in 2024, work was carried out on adapting Security Information & Event Management (SIEM) systems to low-latency requirements and new types of threats. Innovative approaches to securing communication protocols, security monitoring and policy-driven automation solutions were applied to the management of future energy supply grids. The transfer of research results into practice was also intensified as part of dtec.bw projects: For example, the first five sites for the test operation of an energy self-sufficient blackout crisis communication system based on LoRa radio technology were put into operation as part of a cooperation with the Austrian municipality of Neuhaus.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



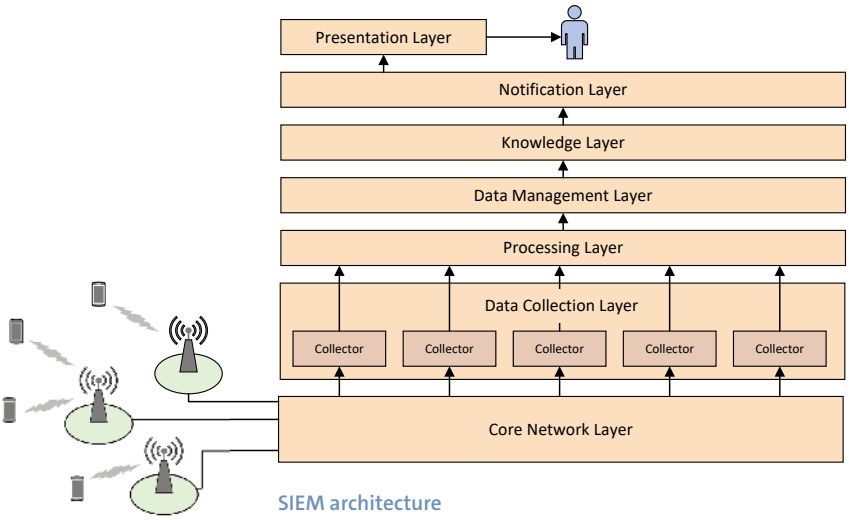
Main research topics of the Professorship of Software and Data Security.

FIG.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK, QUELLE: FI CODE / WOLFGANG HOMMEL

Project 6G-life

Digital transformation and sovereignty of future communication networks

The 6G-life project uses a holistic approach to research innovative concepts in the field of scalable communication, new methods, flexible software concepts and adaptive hardware that support the basic idea of human-machine collaboration. In all research fields, the requirements for latency, resilience, security and sustainability are always addressed in parallel as multidisciplinary topics.



SIEM architecture

6G: Future-ready networks with integrated security

With 5G, the gateway to digitalization in industry has been widely opened. Beyond controlling machines, 5G enables the Internet of Things in real time. However, a significant drawback of 5G communication networks is the limited use of innovative technologies, which restricts their future viability. By integrating novel technologies, the requirements for highly precise services in 6G networks are to be addressed. This, however, brings security-related challenges. Therefore, securing both the communication infrastructure and the communication itself should be considered from the outset in 6G, ensuring a native integration into standards and protocols.

SIEM architecture

As part of the 6G-life project, approaches for a distributed Security Information & Event Management (SIEM) system for 6G networks are being explored and prototypically implemented. In contrast to the current state of the art, the characteristics of 6G networks present new challenges, such as the requirements for energy efficiency in low-power devices, further reduced latencies, and significantly increased data rates. While in-network computing offers new opportunities for decentralized and low-latency correlation and analysis of data compared to conventional hierarchical data aggregation and evaluation, the resulting dynamics—such as changing network topologies and highly distributed software systems—must be considered in the context of IT security analysis and situational awareness visualization.

The SIEM architecture is based on different interconnected layers that work together to collect, process, analyze, and display security-relevant data. In addition to the overall SIEM architecture with concepts for distributed deployment, the work also includes the interfaces for collecting relevant security information from the participating network components and end devices, as well as their situational visualization. Another focus is on the development of scalable mechanisms for processing large volumes of data to meet the increasing demands for data rates and latencies in 6G networks.

Tore Bierwirth

tore.bierwirth@unibw.de

+49 89 6004 7357

https://go.unibw.de/6g-life

Funded by: German Federal Ministry of Education and Research in the program “Souverän. Digital. Vernetzt.” (Confident. Digital. Connnected.)

FIG.: RI CODE / T. BIERWIRTH

Project DEFINE

DC grids for a secure energy supply

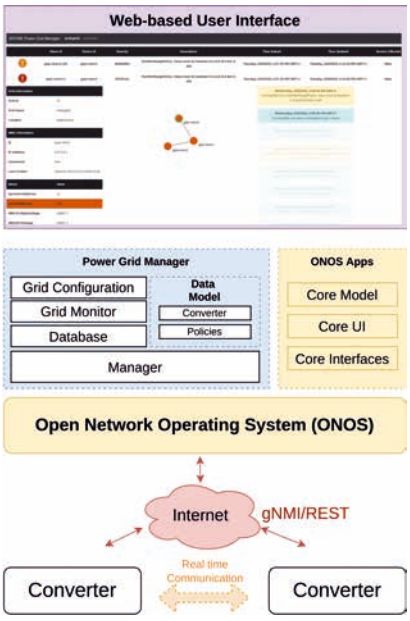
The DEFINE project is researching reliable and secure power grids of the future from the component, container and power grid level through to remote grid monitoring and control from scratch. The aim is not only to ensure a reliable operation, but also to harden the IT infrastructure required to control the grids against attacks.

A two-layer management approach

Converter stations maintain the power grid and actively control power flows to cover power demands, even in the event of a fault. A management system in a grid control center monitors and controls the converter stations. For this purpose, a two-layer approach is being investigated in which, on the one hand, converter stations continuously exchange their state information among each other in a decentralized manner in real time in order to react to changes in power demand and grid faults. On the other hand, a centralized grid control center collects and stores the states of the converter stations in order to prepare a long-term overall view. It detects faults and attacks and automatically contains them.

Power grid control based on SDN

Software-defined networking (SDN) separates the control logic from the network component. ONOS is an SDN management platform that allows the centralized collection of network data and on-demand extension with management applications (apps) in order to assess network data and control the network on this data basis. In DEFINE, this approach is being investigated for power grids and an app for managing modern converter stations and power grids is being designed and implemented. Based on highly flexible protocols such as the gRPC Network Management Interface (gNMI) and REST, key figures from converter stations can be collected as needed. The data is transported via secure communication tunnels (e.g., via TLS). The key indicators are stored centrally and checked for faults or attacks. If a fault is detected, an alarm is displayed on a web-based user interface. The user interface always shows an up-to-date overview of the power grid, the active inverter stations and their current key indicators. The grid view can be opened up both in a central control center and on mobile devices such as tablets. However, the grid control center not only allows the display, but also an automated and/or remote-controlled response to faults and attacks.



An SDN-based control center for modern power grids.

Attack detection and hardening

The management platform must not only implement procedures for attack detection (like event correlation). Protection against unauthorized access or compromise of the grid control center is also a subject of research in order to ensure secure and remotely maintainable power grids of the future.

Dr. Michael Steinke

michael.steinke@unibw.de

+49 89 6004 4825

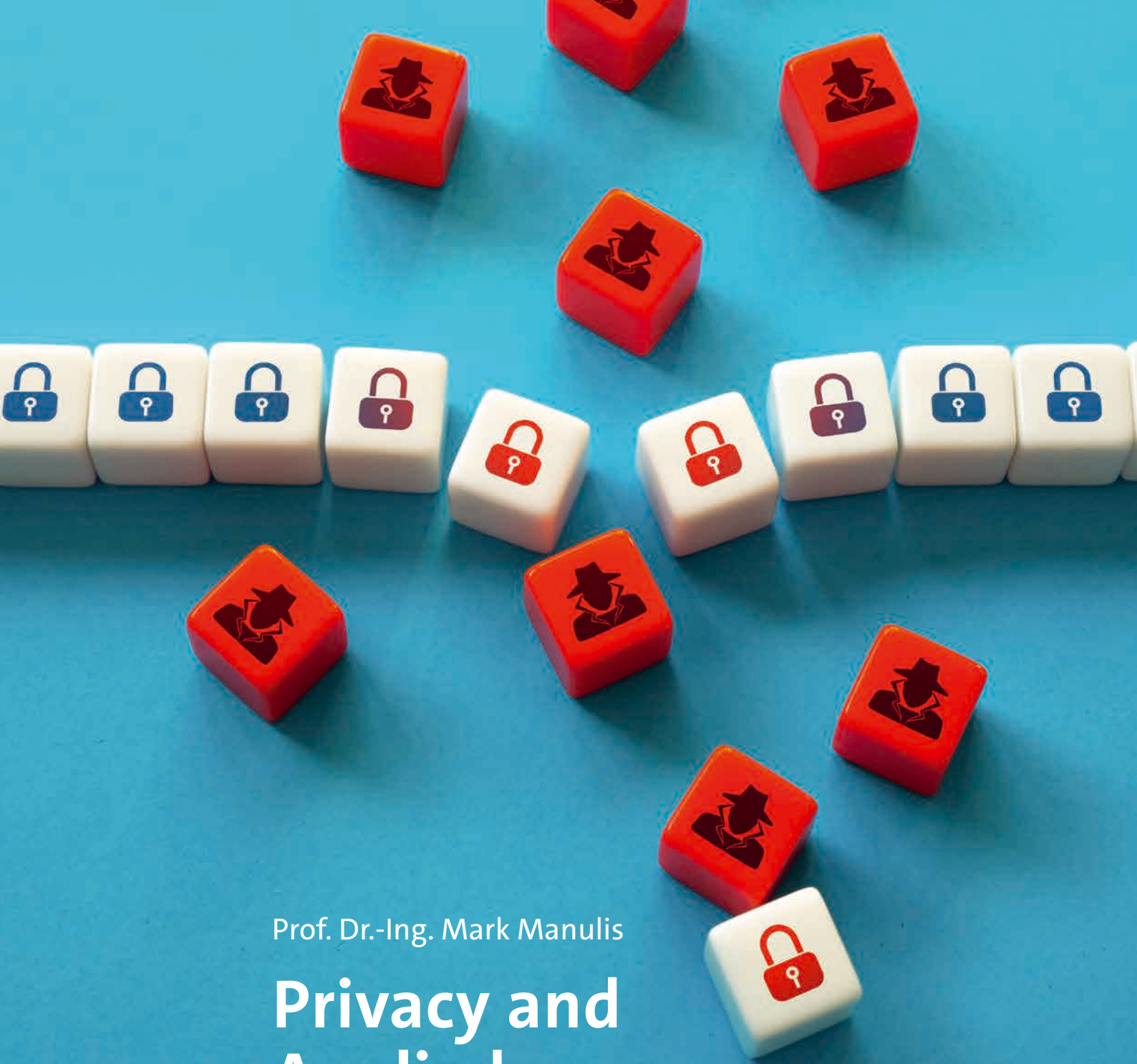
https://go.unibw.de/inf24define

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.

dtec.bw

Funded by the European Union
NextGenerationEU

FIG.: RI CODE / M. STEINKE



Prof. Dr.-Ing. Mark Manulis

Privacy and Applied Cryptography Lab

PACY Lab, led by Prof. Dr.-Ing. Mark Manulis, holder of the Professorship of Privacy, researches technologies for improving privacy based on modern cryptographic methods. The focus is on the design, analysis and development of cryptographic methods for the protection of users, data and messages, as well as their practical use in Web, Cloud, IoT and blockchain applications.

Research foci at the PACY Lab

PACY Lab was established in March 2022 and is part of the RI CODE. Its research staff have in-depth knowledge of cryptography, computer science and mathematics, which they successfully use for foundational and applied research.

The lab explores methods and technologies in the area of Privacy Enhancing Cryptography (PEC), which includes all sorts of cryptographic schemes with extended requirements on confidentiality and privacy.

PACY Lab focuses on the design and practical use of various PEC methods, including advanced encryption and signature schemes and relevant cryptographic protocols. The lab works on the modeling and analysis of their functional properties and protection goals. Dependencies between methods and properties are explored to improve their general understanding and identify new design strategies. PACY Lab develops new PEC procedures and uses them to develop cryptographic protocols for authentication and access control, processing of data and transactions, and secure messaging.

In the design and implementation of new PEC approaches, PACY Lab deploys mathematical techniques that are commonly used in cryptography such as elliptic curves and bilinear maps and now, more often, techniques from lattice-based cryptography in order to realize the desired security against future quantum computers. Other PEC techniques used at PACY Lab include secret sharing and zero-knowledge proofs.

PEC for data: Access control and data processing

Traditional encryption methods can provide data confidentiality but cannot be used directly for processing encrypted data. Modern PEC methods allow a variety of operations on encrypted data without having to decrypt it during processing. PACY Lab is working on functional encryption schemes that offer better flexibility in access control and data exchange as well as enable direct processing of encrypted data in distributed multi-user applications. Ongoing research includes approaches for fully homomorphic encryption and attribute-based encryption as well as cryptographic protocols supporting operations (e.g., search queries) on encrypted data, along with their use in distributed applications.

PEC for users: Authentication and message exchange

Digital signatures form the backbone of modern PKI. With them, users can authenticate themselves or establish end-to-end secure communication channels. The verification of PKI-based signatures reveals a lot of sensitive information, such as identities, public keys and all attributes. PACY Lab is researching advanced signature techniques to combine authentication with anonymity or untraceability. Ongoing research includes attribute-based signature schemes and related concepts behind anonymous credentials schemes. In addition, PACY Lab is researching security protocols for secure and private messaging and for distributed and delegable authentication, for example in connection with the new FIDO2 standard for web authentication.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

FIG.: ADOBE STOCK / A. YALANSKYI; RI CODE

Computing on Encrypted Data with Fully Homomorphic Encryption

Data processing with improved privacy and integrity

Einleitung: Fully homomorphic encryption (FHE) is a groundbreaking cryptographic technique that allows computations to be performed on encrypted data without needing to decrypt it first. In this way, sensitive information can be processed securely, preserving privacy even in untrusted environments. The potential impact of FHE ranges from enhancing data security in cloud computing to enabling privacy-preserving machine learning and many other applications.

Fully homomorphic encryption

Computing on encrypted data with FHE requires complex mathematical structures, such as lattice-based cryptography, to enable operations on ciphertexts that correspond to operations on the plaintexts. Essentially, FHE schemes allow for the evaluation of arbitrary circuits composed of multiple types of gates, making it possible to perform any computation on encrypted data as if it were unencrypted.

Despite its potential, FHE faces significant research challenges. One challenge is the computational overhead, as FHE operations are much slower compared to operations on unencrypted data. FHE storage requirements are also substantial, as the ciphertexts are often much larger than the plaintexts. In addition to improving the efficiency and practicality of FHE, current research is focused on the integrity and verifiability guarantees for FHE computations performed in an untrusted environment.

Our research on the integrity and verifiability of FHE computations

Since 2023, PACY Lab has been looking into security notions available for FHE schemes, their relationships and achievability. Our goal was to develop a common view on the hierarchy of these notions and arrive at the strongest yet achievable definition of security for arbitrary FHE schemes. Clearly stronger notions are those that can protect the integrity of the underlying plaintexts, given that FHE computations on ciphertexts are performed by an untrusted party. Intuitively, the strongest integrity protection results from the ability to verify the result of FHE computations.

In our work published at EUROCRYPT 2024 we came up with the new notion: indistinguishability against verified chosen ciphertext-attack (IND-vCCA). We proved that this notion provides the so-far strongest integrity guarantees for FHE computations and proposed two general transformations that can elevate many of existing FHE schemes to IND-vCCA security level by using so-called zero-knowledge SNARKs. Since its publication our work has influenced the cryptographic community to look at IND-vCCA security of more specialised FHE constructions that are being used in practice.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

FIG.: GENERATED BY DALL·E 3

Fast and Expressive Attribute-Based Encryption

Enabling fast fine-grained access control to encrypted data.

Attribute-Based Encryption (ABE) is a cryptographic technique that provides fine-grained access control to encrypted data. Unlike traditional encryption methods, where access is granted based on the possession of a specific key, ABE allows access based on the attributes of the user. ABE is particularly useful in scenarios where data needs to be shared securely among a large and dynamic group of users.

Challenges in Attribute-Based Encryption

Attribute-Based Encryption (ABE) is a fascinating field with several research challenges. One of the primary challenges in ABE is managing the keys. Each user needs a private key that matches their attributes or access structure. As the number of users and attributes increases, the system needs to handle more keys and more complex access policies. Ensuring that the system remains efficient and scalable is a significant challenge. The encryption and decryption processes in ABE can be computationally intensive. Improving the efficiency of these processes without compromising security is a critical area of research. Of particular practical relevance is the design of expressive ABE schemes that can support complex access structures, such as those involving AND, OR, and threshold gates, which allow for more nuanced and detailed access control to encrypted data.

Building fast and expressive ABE schemes

PACY Lab is working on the design of practical ABE schemes that are capable of handling expressive access policies that can be represented via conjunctive, disjunctive, or any monotonic Boolean formulae to enable practical use in real-world applications. To this end, in collaboration with the University of Surrey (UK), we designed and implemented several efficient ABE schemes with the aforementioned properties. The results of our work appeared in the renowned conference ACM CCS 2025. Our ABE schemes allow the embedding of attributes into user private keys and access policies into ciphertexts, or vice versa, depending on the requirements of a particular application. In addition, some of our ABE schemes enjoy the additional anonymity property, which hides user attributes.

FIG.: GENERATED BY DALL-E 3

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

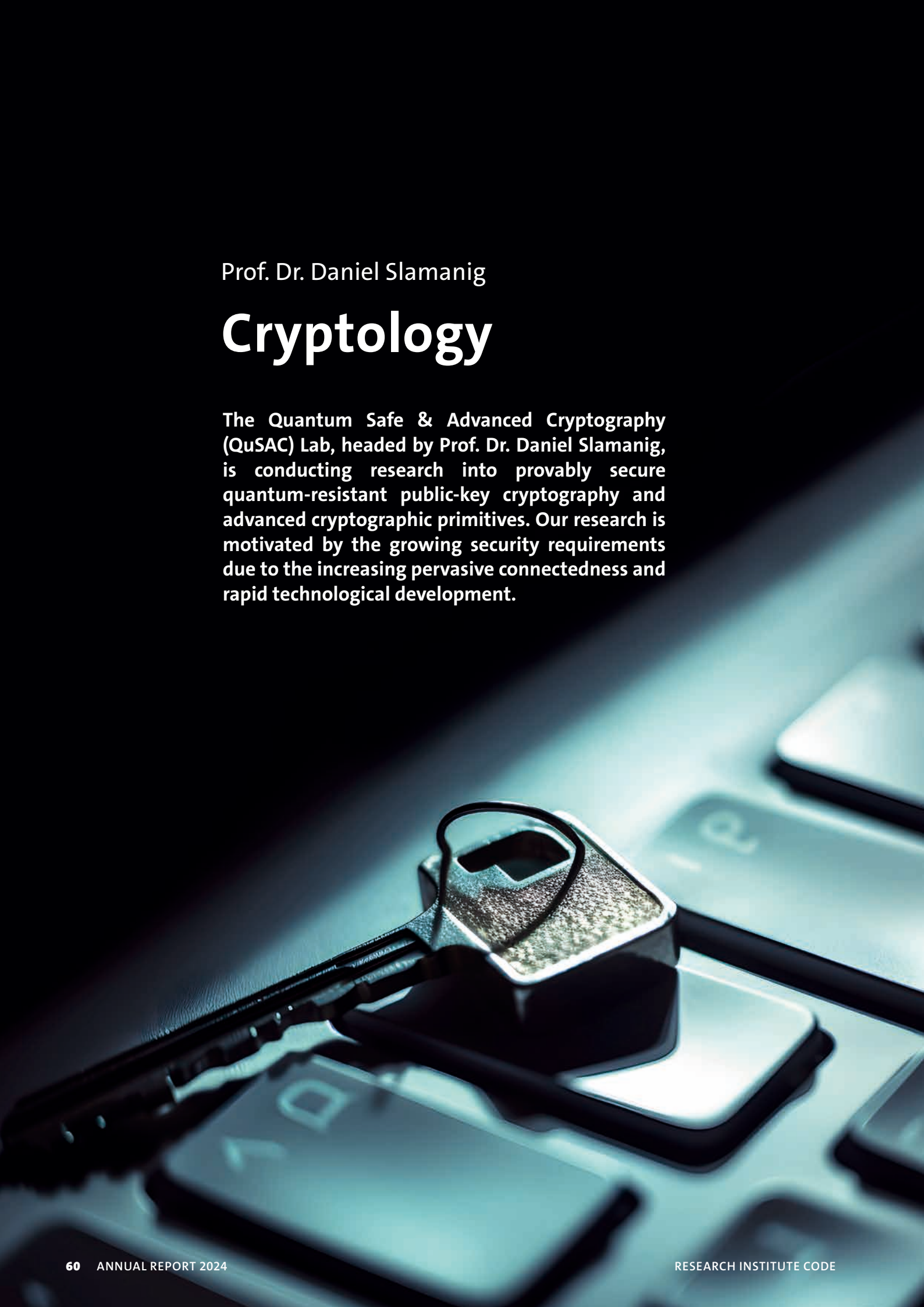
mark.manulis@unibw.de

www.unibw.de/pacy

Prof. Dr. Daniel Slamanig

Cryptology

The Quantum Safe & Advanced Cryptography (QuSAC) Lab, headed by Prof. Dr. Daniel Slamanig, is conducting research into provably secure quantum-resistant public-key cryptography and advanced cryptographic primitives. Our research is motivated by the growing security requirements due to the increasing pervasive connectedness and rapid technological development.



THE QUSAC LAB, led by Prof. Dr. Daniel Slamanig, holder of the Professorship of Cryptology, conducts research in foundations and applications of cryptography. Our primary focus is on quantum-resistant public-key cryptography and advanced cryptographic primitives. We consider both modular constructions based on generic cryptographic building blocks as well as ones based on concrete mathematical assumptions. In doing so, provable security plays a central role in our work.

Relevance of cryptography

Cryptography is at the core of cyber security. It improves security and privacy of most modern digital services and applications, and it is highly relevant to society. However, the complexity of modern scenarios also places high demands on the security and functionality of cryptography.

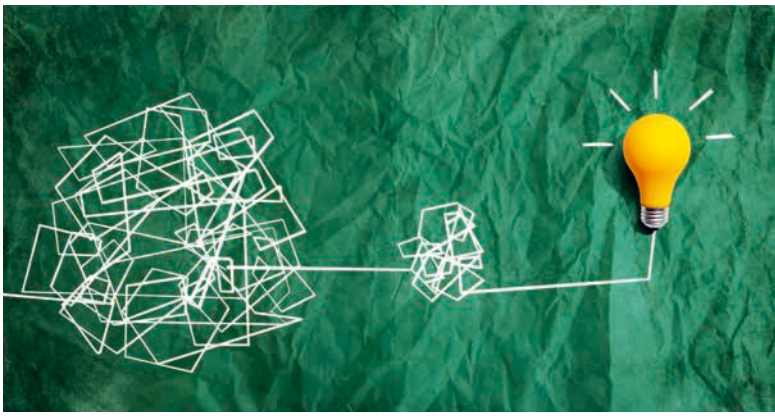
Stronger security properties: Quantum computers and more

Potential advances in the field of quantum computing would make the currently used public-key cryptography insecure. This risk can be mitigated by relying on quantum-resistant (or post-quantum) cryptography. We conduct research on classes of mathematical problems underlying the construction of quantum-resistant schemes (e.g., isogeny-based cryptography) as well as on the design of (advanced) cryptographic primitives. Notably, Prof. Slamanig was involved in the design of the Picnic post-quantum digital signature scheme. It was submitted to what is arguably the most important international post-quantum cryptography standardization project from NIST and reached the final third round there.

Aside from this significant challenge imposed by the quantum threat, some desirable or required security guarantees for modern scenarios are often not provided by basic cryptographic primitives either. Here, for example, we are working on the development of public-key encryption primitives that provide the required strong security properties, as well as on the theoretical foundations of privacy-preserving cryptography.

More functionality and stronger security

Modern applications are increasingly complex and require advanced functionality while at the same time providing high security guarantees. This requires cryptographic mechanisms whose functionality goes far beyond basic primitives. Here, for example, we conduct research on non-interactive zero-knowledge proofs and their succinct variants (so-called SNARKs), which nowadays represent the most widely used advanced cryptographic concept in the real world.



The challenge in cryptography is to solve problems that often seem paradoxical.

Contributions to the academic community

In 2024, Prof. Slamanig was invited to serve on the program committees of various top-tier conferences: the 44th Annual International Cryptology Conference (CRYPTO 2024), the 31st and 32nd Annual ACM Conference on Computer and Communications Security (ACM CCS 2024 and 2025) and the 28th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2025). Moreover, he was invited to serve on the editorial board of the IACR Communications in Cryptology (CiC) journal.

Development of the Research Group

The QuSAC Lab was established in November 2023 and currently hosts two PhD students and a Postdoctoral Reseacher. The group has a strong national and international scientific network, maintains numerous international collaborations and frequently hosts international visitors.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto-en

FIG.: ADOBE STOCK / ANNIKA; ADOBE STOCK / TIERNEY

Advancing Isogeny-Based Cryptography

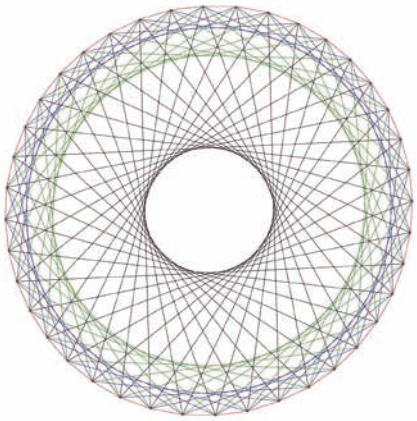
Extending the toolbox of isogeny-based cryptography

Over twenty years ago, Couveignes, Rostovstev, and Stolbunov proposed what is now known as isogeny-based cryptography. This concept is interesting because the problem of recovering a secret isogeny, i.e., a map between two elliptic curves, is considered hard even for quantum computers and the resulting private/public keys are remarkably compact. It represents a very active research field with several cryptographic applications and many interesting connections to number theory.

WHILE ISOGENY-BASED cryptography is a relatively young field, the use of elliptic curves in public-key cryptography dates back to Elliptic Curve Cryptography (ECC) in the eighties; the study of their mathematical properties began even further back in the third century AD with the works of Diophantus and continued, in more recent times, with those of Fermat, Jacobi, Weierstrass, and many others. In simple terms, an elliptic curve is a set of points, whose coordinates satisfy some cubic equation. On this set of points one can define a group structure for which the so-called discrete logarithm problem (DLP) is hard to compute, i.e., practically infeasible for large instances, and thus suitable for cryptography. This is the core idea of ECC. The landmark result due to Shor, however, shows that there exists an efficient quantum algorithm that solves the DLP and thus makes ECC vulnerable to quantum attacks. While the required powerful quantum computers are still hypothetical, today there is a huge push towards transitioning to post-quantum cryptography. This push is also encouraged by the National Institute of Standards and Technology (NIST), which initiated the still ongoing post-quantum standardization project in 2017.

Elliptic curves in a post-quantum setting

In contrast to ECC, isogeny-based cryptography leverages maps between elliptic curves, called isogenies, to realize a trapdoor function for cryptographic use. More precisely, one considers graphs whose nodes represent classes of elliptic curves and whose edges represent isogenies. Recovering a secret isogeny (i.e., a path in the graph) between two given elliptic curves is considered hard even for quantum computers. In 2022, it was shown that departing from this problem, e.g., by providing auxiliary information on how the secret isogeny maps certain points, is dangerous—namely, a devastating attack against SIKE, a competitor in NIST's final round, was demonstrated. This attack, however, did not compromise the core trapdoor function underlying isogeny-based cryptography. Instead, it spurred further research in the field by bringing in novel ideas and techniques.



Toy example of an isogeny graph over a prime field.

Proving knowledge of isogenies

When isogeny-based cryptography is considered for practical applications and more complex cryptographic protocols beyond encryption and signatures, richer functionality is required. For instance, in many cryptographic applications it is required that when a party presents a public key, it also needs to demonstrate that the public key is well-formed. Moreover, in increasingly found decentralized settings, it is typically required that many potentially distrusting parties need to use some common parameters such as specific elliptic curves. Here they need to be sure that no one knows the secret isogeny, which can be viewed as a backdoor. In the QuSAC Lab we are working on designing zero-knowledge proofs for efficiently proving the knowledge of isogenies. This makes it possible to address the above issues and enables many additional applications. Currently, we are particularly interested in realizing such zero-knowledge proofs via arithmetizations using variants of so-called modular polynomials which allow different but equivalent representations of isogenies between elliptic curves.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

FIG.: FI CODE / D. SLAMANIG

Cryptographic Foundations of Privacy-Preserving Authentication

Digital signatures with special properties and zero-knowledge proofs

With the increasing use of online services, the protection of the privacy of users becomes more and more important. This is particularly critical since authentication, as realized on the internet nowadays, typically relies on centralized identity management solutions. Although these are very convenient from a user's perspective, they are quite intrusive from a privacy perspective and are currently far from implementing the concept of data minimization.

FORTUNATELY, cryptography offers exciting primitives such as zero-knowledge proofs and advanced signature schemes to realize various forms of so-called anonymous credentials. Such primitives allow for online authentication and authorization with a high level of built-in privacy protection.

There are different ways to construct anonymous credentials on a technical level. On a high level, a user obtains a signature from an issuer on a set of user attributes. For showing a credential (i.e., performing an authentication), the user then demonstrates possession of such a valid signature from the issuer on a set of attributes that satisfies a certain policy required by the verifier. This can be just revealing a subset of the attributes, or it can be some more complex relation, e.g., the attribute 'birthdate' has to be so that that the holder is above 18 years old. The important point is that the showing does not reveal the original signature from the issuer directly and thus cannot be linked to the issuing, giving strong privacy guarantees. Also, what is revealed during the showings is unlinkable.

Specific signature schemes

One way to construct anonymous credentials is to rely on specific signature schemes. Members of the QuSAC Lab have proposed a new paradigm of signatures called equivalence class signatures. These are signatures that allow to randomize signatures and support a controlled public randomization of a signed message without invalidating the signature. This concept was later extended to mercurial signatures that additionally support key randomization. The latter can be used to construct anonymous credentials with delegation capabilities. Recently, members of the QuSAC Lab have investigated how to construct such schemes with strong unlinkability properties. Unfortunately, these concepts seem to inherently require a rich algebraic structure, and it is so far unclear whether or how they can be translated to the post-quantum setting. To nevertheless work towards a post-quantum anonymous credentials, the QuSAC Lab has recently started investigating the construction of other specific signature schemes, and in particular blind signatures from isogeny-based assumptions.

Nowadays, authentication methods that are "privacy-unfriendly" are still widespread.

FIG.: ADOBE STOCK / KIATTISAK

Zero-knowledge proofs

A second and more generic way is to construct anonymous credentials from any signature scheme, e.g., standardized and widely deployed ones like the Elliptic Curve Digital Signature Algorithm (ECDSA), combined with a non-interactive zero-knowledge (NIZK) proof system. Recent advances in the design of very compact NIZK proofs, so called zk-SNARKs, make the construction of such anonymous credential schemes practically feasible, and there are first very recent works by teams from Google and Microsoft who plan to deploy them practically. Again, when looking into post-quantum constructions there are many challenges to be solved. The QuSAC Lab is working on the foundations of such constructions, in particular the design of post-quantum zk-SNARKs.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

Prof. Dr. Arno Wacker

Privacy and Compliance

Don’t just teach data privacy and compliance, live it!

ONE OF OUR MOST important goals is not only to research and teach data protection and IT security, but also to live them in everyday life. This is the only way to communicate these topics to students in a convincing and authentic way. We also want to show the general public that technologies that promote data protection can be integrated into everyday life, both in the private and business spheres.

Teaching

In the professorship, teaching is divided into data protection, privacy-enhancing technologies, pentesting, cryptology and secure networks and protocols. Data protection and privacy enhancing technologies teach students, among other things, what privacy is and why it is important both for individuals and for democratic societies. Pentesting covers the testing of individual systems, complex IT services, and entire IT infrastructures, as well as practical attack variants based on tried and tested best practice documentation. Cryptology teaches the basics of cryptography as well as knowledge of the various methods for secure data transmission in modern communication networks.

Research

A particular focus of the professorship is on methods and mechanisms to support privacy and data protection and is divided into three different research areas:

- Privacy-supporting mechanisms aim at strengthening the privacy of individuals as well as researching communication rules for the Internet age.
- Increasing IT security awareness is concerned, among other things, with the area of self-data protection. To this end, the professorship develops and researches methods and tools to increase security awareness in the development of software tools and in their use.

- The cryptanalysis of classical ciphers investigates the field of classical encryption methods with the help of modern (meta-)heuristic methods. Among other things, the efficiency of the analyses and the security of the algorithms are examined.

Knowledge transfer

A particular concern of our professorship is to train, educate, and inform interested members of the public about IT security issues. We pursue this goal with lectures and workshops on topics such as pentesting, secure email traffic in everyday life and the detection of security vulnerabilities.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

FIG.: ISTOCK / MATEJMO; RI CODE / DATCOM

Strong Authentication with UniBwM-ID and SecureID

More security and convenience with the introduction of the UniBwM-ID.

Since April 2024, the University of the Bundeswehr Munich has been offering a new two-step login solution: the UniBwM-ID with passkeys and the particularly secure UniBwM-SecureID with hardware-based keys. The goal of the project was to combine high IT security standards with maximum user convenience.

THE PROJECT WAS initiated by the university's IT Service Center in April 2024. Under the leadership of Professor Wacker, who holds the Professorship of Privacy and Compliance and also heads the IT Service Center, a well-conceived concept was developed that combines stringent security requirements with practical user-friendliness. Professor Wacker provided the core idea, the overall concept, and key parts of the architecture, while his team at the IT Service Center managed the operational implementation. The project was successfully completed on schedule for the start of the trimester on October 1, 2024.

With this project, the university aimed to replace the traditional, increasingly insecure username-and-password approach. The new authentication architecture is designed to render stolen credentials useless to attackers. Two distinct security levels were developed: The UniBwM-ID enables the use of passkeys for "standard" services such as ILIAS or GIT, while the UniBwM-SecureID is tailored for highly sensitive areas where users manage and update their university access credentials. For these sensitive services, the use of hardware-based security keys remains mandatory.

A key aspect of the project was to combine security and convenience. Passkeys based on the FIDO2 standard enable password-free logins, with authentication tied to the device, for example via Apple Face ID or Windows Hello. The UniBwM-ID allows quick and easy access to university services without administrative privileges, such as ILIAS. For services with highly sensitive data, such as user administration at nutzer.unibw.de, the UniBwM-SecureID is required, which mandates the use of hardware-based security keys like YubiKeys. This combination of passkeys and hardware security keys ensures comprehensive protection of login credentials against phishing and data theft.

Authentification at the UniBW M: UniBwM-ID and UniBwM-SecureID combine convenience and security.

With this authentication solution, the professorship was able to realize its motto: "Not only teach data protection and compliance, but also live it." The modern security architecture prevents logins without hardware keys in sensitive areas, while simultaneously offering a convenient solution for "standard" services. Thanks to the expertise of the Professorship of Privacy and Compliance, the IT Service Center successfully established a future-proof authentication solution at the university with the UniBwM-ID. By October 2024, all university members were equipped with a YubiKey, and login via username and password for the affected services was completely phased out as of October 1, 2024. This project represents a significant milestone in the university's IT security, demonstrating how theoretical knowledge can be effectively applied in practice —a prime example of the close connection between academic research and operational implementation.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

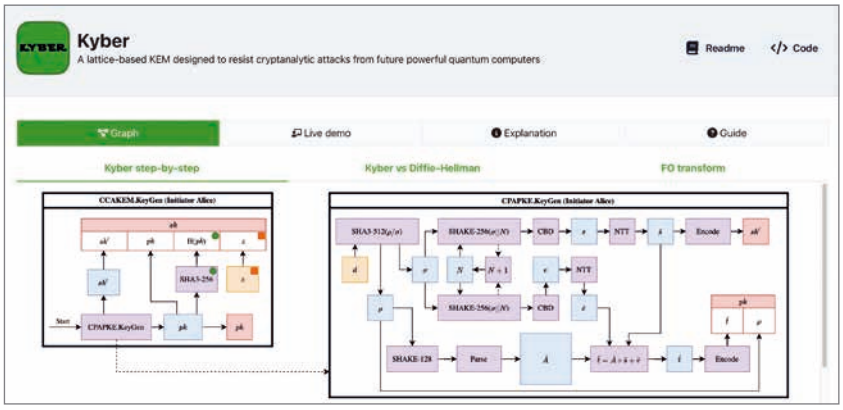
FIG.: RI CODE / A. WACKER

Project CrypTool

New web apps for cryptography and cryptanalysis

The CrypTool project (www.cryptool.org), with its collection of software applications and teaching materials on the subject of cryptography built up since 1998, was relocated in 2023 from the University of Siegen to the Professorship of Data Protection and Compliance of Professor Wacker. In addition to maintaining the existing collection, several web apps were newly developed, public relations work was conducted, and connections were made to find focal points for the future direction of the project, targeting the German Armed Forces as a user base.

IN ADDITION TO smaller apps, such as the Enigma app, which a student from the University of the Bundeswehr Munich developed as part of his Bachelor's thesis (https://www.cryptool.org/en/cto/enigma/), we had the following larger subprojects:



Interactive Kyber WebApp

1. Learning Program

A new learning web app tailored to the cryptography section of the new Bavarian high school curriculum has been developed: https://learn.cryptool.org

The app has been in public beta since November 2024. In coordination with the Bavarian State Institute for School Quality and Educational Research in Munich, the app will potentially be included in the Curriculum Information System via a link after processing feedback from schools. This could lead to every student who completes high school in Bavaria to get to know our app and thus CODE.

2. AI

AI has been successfully applied in the CrypTool project for the cryptanalysis of both classical and historical ciphers by determining the encryption method when only ciphertext is available. Custom models (neural networks) were trained for this purpose. This approach works quite well with a limited number of around 50 ciphers and has also been made publicly accessible through the NCID app within CrypTool Online (https://www.cryptool.org/en/cto/ncid/). Our current research is testing the limits of existing LLMs by using code-based prompt engineering instead of training custom models.

3. Post-Quantum Cryptography

The key encapsulation mechanism previously known as Kyber was standardized by NIST in August 2024 (https://csrc.nist.gov/pubs/fips/203/final). A CrypTool web app that explains this mechanism using interactive graphics has been under development since 2023 and is currently being revised to contain the latest changes from NIST. It will soon be available as a CrypTool Online app: https://www.cryptool.org/de/cto/kyber/.

Prof. Dr. Arno Wacker
arno.wacker@unibw.de
+49 89 6004 7325
www.cryptool.org

FIG.: RI CODE / CRYPTOOL / A. WACKER

Prof. Dr. Gabi Dreo Rodosek

Communication Systems and Network Security

The professorship deals with the use of generative AI/ML in network security and social media analytics, software-defined networking, 5G/6G networks, and the detection, assessment and mitigation of cyber risks.

Project 6G-life

Digital transformation and sovereignty of future communication networks

6G-life drives cutting-edge research for 6G communication networks with a focus on human-machine collaboration. 6G-life provides new approaches for sustainability, security, resilience and latency and will sustainably strengthen the economy and thus digital sovereignty in Germany.

THE PROJECT, coordinated by TU Dresden and TU Munich, engages approximately 162 principal investigators, 162 researchers and 19 startups, supported by a €70 million funding initiative. Here we address the network security research area.

6G network security is essential in building high-trust cyber-physical systems. The research explores diverse aspects of 6G network security, emphasizing the evolving threat landscape, advanced anomaly detection techniques, the application of a Zero Trust Architecture (ZTA), and Trusted Execution Environments (TEEs).

A comprehensive threat analysis has been conducted, addressing 6G-specific vulnerabilities, particularly in the supply chain, and emerging attack vectors driven by artificial intelligence (AI) and machine learning (ML). To enhance threat detection, AI-powered anomaly detection techniques, such as Temporal Graph Neural Networks (TGNNs), are explored for their ability to identify deviations in dynamic network environments. Additionally, the potential of Large Language Models (LLMs) for enhancing network security with respect to automated threat and anomaly detection has been analyzed.

The solutions from 6G-Life will enable new forms of human-machine interaction.

Security-by-Design remains a core principle, particularly within Service-Based Architectures (SBAs), ensuring authentication, authorization, and robust encryption for all network interactions. Additionally, the roles of crucial components like Network Repository Function (NRF), Service Communication Proxy (SCP), and Network Exposure Function (NEF) are analyzed for their role in enabling secure operations.

Prof. Dr. Gabi Dreo Rodosek

gabi.dreo@unibw.de

+49 89 6004 7360

https://6g-life.de

Funded by: German Federal Ministry of Education and Research (BMF) in the program “Souverän. Digital. Vernetzt.” (Confident. Digital. Connnected.).
Joint project 6G-life, project identification number: 16KISK002.

FIG.: ADOBE STOCK / DENIS PUTILOV; ADOBE STOCK / SERGEY NIVENS

Prof. Dr. Ulrike Lechner

Information Systems Research Group

The Information Systems Research Group, led by Prof. Dr. Ulrike Lechner, approaches security from an interdisciplinary perspective, considering technological, organizational and human factors. A key focus of the group is the development of educational games in the field of cybersecurity, aiming to raise the awareness of risks, mitigation strategies, and incident response.

Project CONTAIN

Effective responses to threats from the digital space

The CONTAIN research project aims to enhance the effectiveness and efficiency of responses to threats in the digital space. The project focuses on ransomware, which can impact personal devices, corporate networks with operational information systems, production facilities, or partners within the supply chain.

CONTAIN IS A German-Austrian research initiative that brings together an interdisciplinary consortium to develop and evaluate innovative concepts and strategies for mitigating and responding to ransomware attacks.

The CONTAIN research approach

To improve resilience against cyberattacks, CONTAIN develops scenarios, serious games and simulations, and conducts a demonstration exercise. The project is designed in close dialogue with end users. Three key scenarios are examined:

1. Ransomware attacks on personal devices
2. Ransomware incidents in corporate networks
3. Ransomware threats in digital supply chains

Serious games: Awareness and preparedness for action

The serious games developed within CONTAIN aim to raise awareness of incident response and business continuity while also preparing participants for effective decision-making during crisis situations.

A Question of Security: This game focuses on ransomware attacks on personal devices. Players assume different roles—such as a family member, friend, supervisor, IT security officer, data protection officer, or law enforcement representative—and reflect on the questions and actions they would consider in response to an attack.

Operation Raven: This serious game simulates a ransomware incident in the network of a critical infrastructure operator. Players develop strategic responses in a turn-based format to prevent the takeover of the network by ransomware.

CopyCat: The CopyCat game addresses threats in the digital supply chain, specifically focusing on cloud-based attack vectors and the shared responsibility of security measures in cloud services. It is designed for software developers in the industrial sector.

Hack-Me-Not: Aimed at employees and decision-makers in the logistics sector, this game raises awareness of supply chain threats and allows participants to develop and test security measures.

Key research outcomes

As part of CONTAIN, a framework for IT security is being developed, specifically targeting small and medium-sized enterprises (SMEs). The research findings and developed strategies will be demonstrated in a federated exercise. Detailed information and research outcomes can be found on the project website.

Project partnership and funding

CONTAIN is part of Germany's Civil Security Research Program (SIFO) and Austria's KIRAS security research program. Companies and government agencies from both countries collaborate to develop innovative solutions for increasing cyber resilience.

The project consortium extends its gratitude to the German Federal Ministry of Education and Research (BMBF, FKZ 13N16581-13N16587), the German Federal Ministry of Finance (BMF, FO999902707), and the Austrian Research Promotion Agency (FFG) for their support and funding.

Prof. Dr. Ulrike Lechner

ulrike.lechner@unibw.de

+49 89 6004 2504

www.contain-projekt.de

Funded by: German Federal Ministry of Education and Research (BMBF), German Federal Ministry of Finance (BMF), Austrian Research Promotion Agency (FFG)

FIG.: ADOBE STOCK / USAMA

Jun. Prof. Dr. Maximilian Moll

Operations Research — Prescriptive Analytics

Jun. Prof. Moll's research focuses, on the one hand, on reinforcement learning, where he is particularly interested in the possible combinations with classical operations research as well as the applications in prescriptive analytics and prescriptive intelligence. On the other hand, he is researching the interfaces of quantum computing with optimization and machine learning.

Quantum Machine Learning for the Future Combat Air System

Assessing the potential of quantum machine learning as an addendum to classical AI tools

As quantum computers advance, they promise to tackle problems that are currently infeasible for classical systems, unlocking new opportunities in data analysis, optimization, and pattern recognition. In today's data-driven world, where machine learning powers technologies from healthcare to artificial intelligence, this study investigated quantum machine learning (QML) as a forward looking alternative to classical machine learning (ML).

IN A LARGER project, IBM is creating the AI backbone for the future combat air system, which provides a central infrastructure and algorithmic tools for analyzing data. This one-year study was tasked with investigating whether QML could be a promising future addendum to the classical tools offered.

The project consisted of a comprehensive survey of the state of the art and experiments on IBM quantum hardware for a more targeted analysis. In addition, an introduction to quantum computing was written along with an overview of existing algorithms and hardware options.

Quantum machine learning research

Like classical ML, QML can be categorized into approaches with or without neural networks, distinguishing those using quantum variational circuits (QVCs) as quantum analogues of neural networks from those that do not. The non-QVC literature primarily focuses on developing quantum versions of classical ML algorithms, though many rely on a non-existent Quantum RAM for speedups.

The QVC literature primarily explores the replication of neural network architectures. While various applications are addressed, the majority of studies focus on image classification. QVCs frequently demonstrate competitive performance against classical neural networks and, in some cases, surpass them.

Switching from Bit to Qbit creates the potential of benefits in QML.

Exploring quantum variational circuits: Experiments on IBM hardware

In the second part of the project, experiments were conducted on the problem of time series classification based on a public dataset suggested by IBM. Apart from project relevance, the experiments have additional scientific value as the survey showed that quantum time series classification is drastically under-researched. Thus, a comparative analysis of two classical neural network-based methods against their hybrid quantum variants was conducted. An additional focus was the comparison of performance on perfect simulators against real quantum hardware.

While quantum algorithms demonstrated performance comparable to their classical counterparts in simulations, their efficacy significantly deteriorated when deployed on real quantum hardware. This finding contrasts with previous studies on non-time series tasks, where performance remained stable. Additionally, scalability remains a critical challenge, as single evaluations on quantum machines required several hours to complete.

In conclusion, QML exhibits strong potential for applications across various domains, benefiting from reduced parameter requirements and competitive task performance. However, significant hardware-related challenges persist, with the most pressing issue being the susceptibility of current quantum hardware to noise.

Jun. Prof. Dr. Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

FIG.: ADOBE STOCK / TIERNEY; SHUTTERSTOCK / PRODUCTION PERIG

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

We develop intelligent methods to tackle real-world data challenges, such as imbalances and evolving datasets, and to promote social good. Our research focuses on responsible AI (fairness, explainability, robustness), adaptive learning and generative AI to create new solutions, including generating data to enhance AI quality. Applications span key areas such as education, agriculture, banking and engineering.

THE Artificial Intelligence and Machine Learning (AIML) group focuses on researching and developing intelligent algorithms that address real-world data challenges and contribute to the societal good. Our work is driven by three core questions: How can we build intelligent machines for the real world? What kind of intelligence do we aspire to create? Can AI exhibit creativity—and how can we harness this creativity for meaningful applications? Our research focuses on responsible AI (fairness, explainability, robustness), adaptive learning, and generative AI. These areas span multiple application domains, including education, social networks, banking, agriculture, manufacturing, and engineering.

Research highlights

In 2024, our group made significant contributions to the AI field, with impactful advancements in theory and applications. Highlights include TABCF, a novel method for counterfactual explanations for tabular data using a transformer-based VAE (presented at ACM ICAIF 2024) and a transparent neighborhood approximation method for text explanations (presented at IEEE DSAA 2024). We also developed FairBranch, a bias-aware multi-task learning method to mitigate negative and bias transfer across tasks (presented at IEEE IJCNN 2024), and a method for fair graph clustering using contrastive regularization (presented at PAKDD 2024).

Project highlights

We achieved significant milestones across several projects, demonstrating our commitment to impactful, domain-specific AI solutions. The EU project MAMMOTH advanced fairness-aware AI by developing bias mitigation tools across diverse data types and multi-dimensional identities, with applications in finance and identity verification. The EU project STELAR developed a Knowledge Lake Management System for FAIR and AI-ready data, piloted in the agrifood sector. The DFG project HEPHAESTUS enhanced adaptive process planning for 5-axis milling, improving accuracy and reducing manual adjustments. Finally, the DFG CRC1463 concluded successfully, integrating simulations and AI to optimize the design and operation of offshore megastructures. Our contributions include a novel dataset for the data-driven conceptual design of offshore jacket substructures (published in *Ocean Engineering*), highlighting the importance of high-quality data in engineering.

FIG.: ADOBE STOCK / LUCEGRAFIAR; ADOBE STOCK / STARLIGHT

International Presence

Our group promoted its work at international and regional forums, reaching diverse audiences. A key event was the AI Fairness Cluster Inaugural Conference & Workshop on AI Bias in Amsterdam, which brought together over 50 institutions to address AI bias. At the Versus Festival in Austria, we contributed to the panel "AI vs. Mensch", and at the "Intl. Conf. on Web Engineering" in Finland, we joined the panel "Weaving an Ethical and Human-Centric Web". Prof. Ntoutsi served as Program Co-Chair for ECML PKDD 2024 in Lithuania, one of the leading conferences in machine learning, and co-organized the ReAI Workshop at SETN in Greece, discussing the future of AI. Further, we offered an advanced course on "Fairness and Explainability—Models, Measurements, and Mitigation Techniques" at ESSAI 2024 in Athens and led a summer vacation workshop for girls as part of the UniBw M's "Strong Girls do MI(N)T!" program, introducing them to responsible AI.

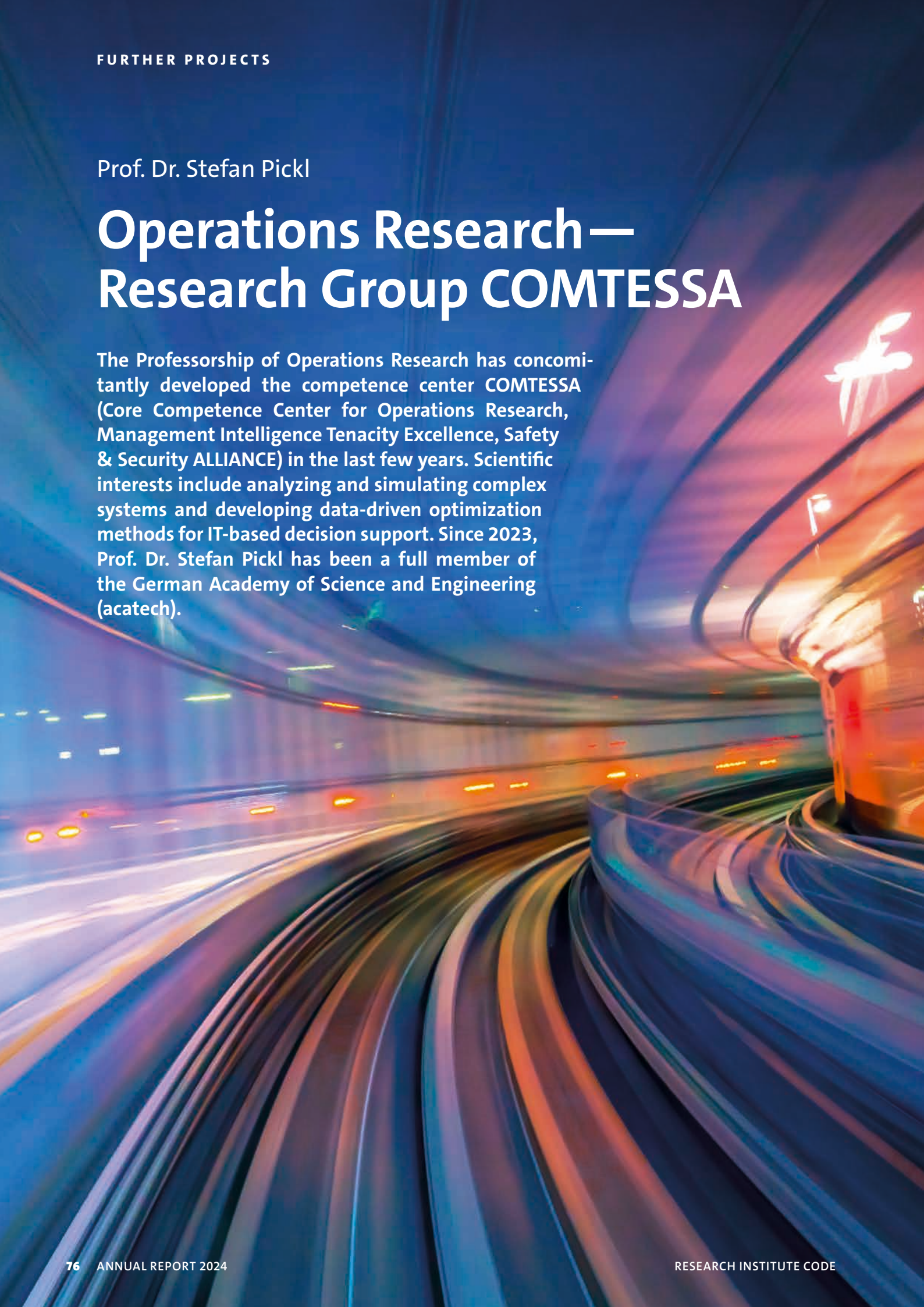
Looking forward to 2025, we are focused on addressing the complex challenges posed by rapid technological, societal, and legal developments with innovative and responsible AI solutions.

Prof. Dr. Eirini Ntoutsi
eirini.ntoutsi@unibw.de
+49 89 6004 7420
www.unibw.de/aiml-en

Prof. Dr. Stefan Pickl

Operations Research — Research Group COMTESSA

The Professorship of Operations Research has concomitantly developed the competence center COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) in the last few years. Scientific interests include analyzing and simulating complex systems and developing data-driven optimization methods for IT-based decision support. Since 2023, Prof. Dr. Stefan Pickl has been a full member of the German Academy of Science and Engineering (acatech).



Project REAVRS

Revealing existing attack vulnerabilities in the rail system

Based on the increasing use of digitalization aspects such as big data, IT, etc., the railroad system has an increased vulnerability to attacks from third parties. A general approach to standardized attack security has not yet been established. REAVRS is developing a complex vulnerability model of the rail system in order to subsequently develop intelligent (AI-based) measures against both physical and cyber threats.

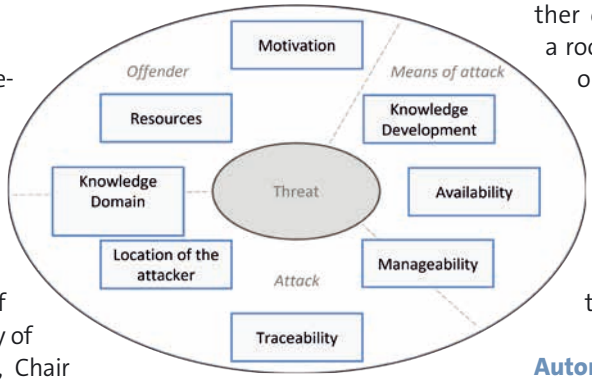
Objective

The objective of the REAVRS research project of the German Center for Rail Transport Research (DZSF) is to determine the current vulnerability of the German railroad system. The participating partners in the project are the University of the Bundeswehr Munich, Faculty of Computer Science—Institute 1, Chair for Operations Research, the COMTESSA research group (project management) in cooperation with the CODE research center, as well as the IVE Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), CreaLab GmbH, and the Institute of Transport, Railway Construction and Operation (IVE) at the TU Braunschweig.

The project is divided into the following topics:

- Identification of existing attack potentials and scenario development
- Complex root cause analysis
- Intelligent risk analysis and assessment
- Development of recommendations for preventive measures
- Automation of the threat model

As part of the project, an initial identification of existing weaknesses and a comprehensive risk analysis of the causes of these vulnerabilities are carried out. On this basis, security measures and the necessary implementation strategies can be derived and recommended.



Identification of parameters for the threat.

OR-based system analysis

A functional mapping of the (German) railroad system is developed, followed by precise research into attacks that have occurred and a description of typical contexts. Attack possibilities and threat scenarios are being systematized and a threat identification is created on the basis of an OR-based system analysis.

Cyber vignettes and attack scenarios

After preselecting the points of attack, these are then developed into exemplary model vignettes. When systematizing the means of attack, a general distinction is made between physical vignettes and cyber vignettes. After extensive research, more than 500 physical and almost 1000 possible cyber attacks were identified. A selection of representative vignettes is being evaluated. The associated attack scenarios are further described as examples so that a root cause analysis can be carried out. In the final step, the developed methodology is embedded in both a convenient IT-based environment for better decision support as well as in a comfortable management cockpit with reachback functionalities (Comtessa Suite).

Automation and "Safety & Security" living lab

The subsequent results of the root cause analysis—the individual values of the respective vignettes—are displayed in a so-called fishbone diagram for selected GSM-R modem cyber vignettes: This detailed root cause analysis is incorporated into the subsequent risk analysis. An automated version of the threat model and a supporting management cockpit are currently being created in order to develop a "Safety & Security" living lab of the German railroad system at HOLM.

Prof. Dr. Stefan Pickl

stefan.pickl@unibw.de

+49 89 6004 2400

https://go.unibw.de/reavrs

Funded by: German Center for Rail Traffic Research (DZSF)

FIG.: ADOBE STOCK / NAKA; PICKL S., BUCHETMANN B., ALONSO VILLOTA M., LORETH T. UNIVERSITÄT DER BUNDESWEHR MÜNCHEN; SIEFERT., STUTE F. TU BRAUNSCHWEIG; JELINSKI M. IVE MBH, HANNOVER; NEUBECKER K. A., SCHMITZ W. CRE-ALAB GMBH, FELDKIRCHEN-WESTERHAM.

PD Dr. Corinna Schmitt

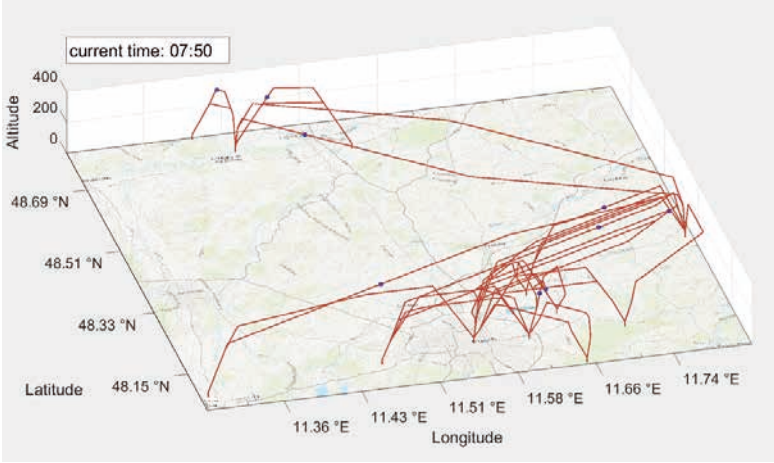
Project AMIUS

RI CODE is a partner in the AMIUS project—Air Mobility Integration U-space—with the aim of creating the first integrated Bavarian U-space connecting the city of Ingolstadt with Manching Airport. Together with regional industrial partners, corresponding communication concepts and model-based feasibility approaches are being specified and an initial prototype developed.

THE AMIUS PROJECT is one of the numerous projects funded by the Bavarian State Ministry of Economic Affairs, Regional Development and Energy as part of the "Air Mobility" funding program. The aim is to create the first integrated Bavarian U-space connecting the city of Ingolstadt with Manching Airport. The consortium is made up of regional industrial partners (i.e., Airbus Defence and Space, Airbus Urban Mobility, and SkyFive) and academic institutions (UniBw M/RI CODE and TU Munich). RI CODE is supported by expertise from the associated partner TU Hamburg—Institute of Air Transportation Systems (ILT).

In addition to the activities described here, this U-space is available as a real test field for use by Bavarian companies in industries of electric vertical take-off and landing aircrafts (eVTOLs, such as air taxis or helicopters) and unmanned aerial systems (UASs, such as drones). The project investigates how a U-space based on digital services can integrate today's air traffic, filled with processes and technologies, with future deployment scenarios of UASs and eVTOLs in a common airspace. To this end, the necessary air traffic management functions for safe, integrated and efficient operations will be provided and demonstrated through the U-space services defined by the European Aviation Safety Agency (EASA).

Based on these digital services, flight routes and simulations for the corridors of the Ingolstadt—Manching—Munich metropolitan area are being planned. These practical demonstrations will be supported by corresponding scientific model-based preliminary investigations, multimodal simulations with various transportation systems, feasibility studies and cost analyses by the participating universities. To ensure the safe and efficient integrated operation of UASs, eVTOLs, and general aviation in the future, new traffic concepts are required. To this end, the existing airspace management system must be supplemented by an integrated UAS Traffic Management System (UTM) and thus expanded to include the dimension of previously uncontrolled airspace. The focus is on the design and technical implementation of the demonstrator with a UTM system and corresponding ground infrastructures, supplemented by innovative communication technologies and a central control station. The project is also investigating how the data flow between the participating airspace users and the storage of relevant data can be secured against unauthorized external interference using various measures.



Simulation of flown trajectories in the AMIUS U-space Ingolstadt—Munich.

Together with the ILT, RI CODE is pursuing two objectives in the field of UAS research as part of the joint project: (1) On the basis of a scalable model-based approach in close connection with real test approaches of the project partners, reliable statements are to be made on how to establish the necessary command and communication infrastructure for urban air mobility. (2) Solutions for secure cloud-based data storage during operation and over the lifecycle will be developed to reduce the delay in data analysis and communication. The developed simulations, cost and infrastructure estimates, as well as the cloud concepts and standard analyses, will be made available for the technical development of a prototype.

PD Dr. Corinna Schmitt

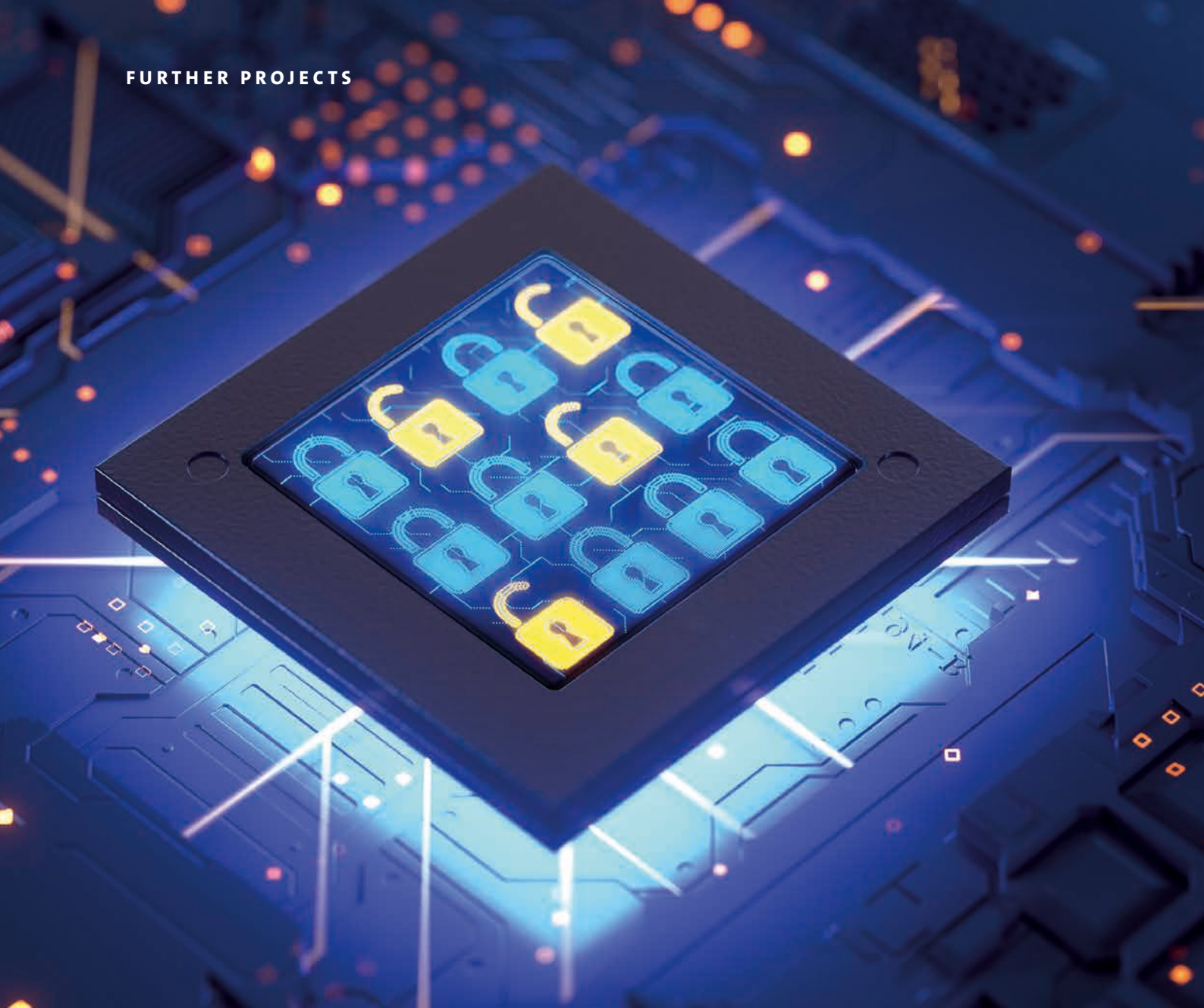
corinna.schmitt@unibw.de

+49 89 6004 7314

https://go.unibw.de/amius

Funded by: Bavarian State Ministry of Economic Affairs, Regional Development and Energy as part of the "Air Mobility" funding program (No. ROB-2-3410.20-04-11-15/HAMI-2109-001)

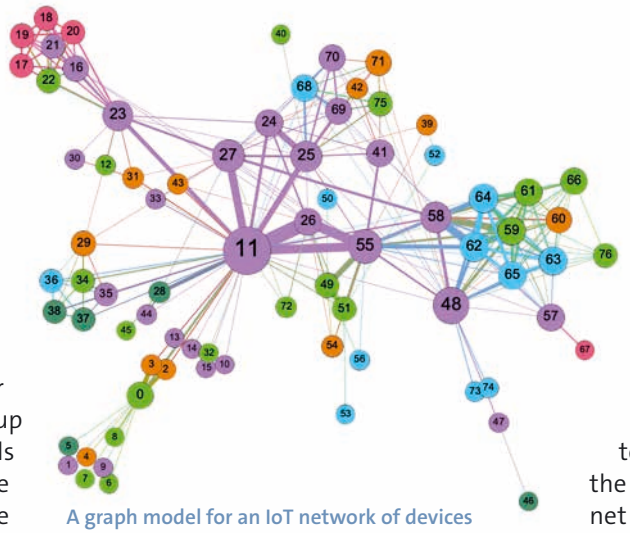
FIG.: AIRBUS HELICOPTERS / CHRISTIAN KELLER; AMIUS REPORT



Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

The research group FOMSET applies formal methods to achieve IT security in the domain of embedded and cyber-physical systems. This involves methods such as the formal software verification of operating systems and graph-theoretical modeling of IoT networks. The research is conducted in PhD projects and in cooperation with industry partners.



A graph model for an IoT network of devices with different properties.

THE GOAL OF the research group of Prof. Dr. Gunnar Teege is to increase the use of formal methods for securing IT systems. The group examines different kinds of systems and studies the methods which are applicable to achieve specific security properties for them.

Formal verification of system software

System software, such as device drivers and other operating systems components, is often crucial for the security of the complete IT system based on it. Therefore, the formal confirmation that it does not contain errors or vulnerabilities is of high relevance for the whole system. At the same time system software is still implemented today in programming languages such as C or C++ or even assembly languages, which makes the application of formal verification methods difficult and expensive.

The goal of the working group is to increase the degree of automatization for formal proofs about system software supported by mathematical proof assistants like Isabelle or Coq.

Attesting cloud systems based on microkernels

Users of a cloud system must be able to rely on the system to protect security properties for their applications, such as integrity and confidentiality with respect to other users. This requires that the cloud system does not allow violations of these properties and that it can prove this to the user by transmitting manipulation-safe evidence about it (“attestation”). The research in the group investigates the realization of such evidence based on microkernels, such as the formal verified seL4 kernel.

Graph-based modeling of malware infections in IoT networks

The huge number and often weak security facilities of the single devices in IoT (Internet of Things) networks mostly prevents the application of conventional measures, such as security software updates, for securing such networks against attacks. The research in the group investigates graph-based models of the devices and their connections to identify security relevant structures in the networks and to exploit them against attacks. For this purpose, it transfers methods to IoT networks which have been developed and applied for information propagation in social networks and also for the spreading of infectious diseases.

Securing vehicular networks using blockchain technology

Interconnected vehicles exchange information among each other and with the traffic infrastructure. This exchange is most effective if as many instances participate in it as possible. At the same time, a large number of participants increases the risk of attacks on integrity, availability, and possibly confidentiality of the information. Blockchain technology has been developed for cryptocurrencies and is also applied for the tracking of goods. For its application in vehicular networks it must be modified and adapted. The research in the group investigates necessary modifications which make blockchain technology applicable to achieve verifiable security properties for vehicular networks.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

+49 89 6004 3353

www.unibw.de/fomset

FIG.: [M] SHUTTERSTOCK / BLUE ANDY; ISTOCK / MATEJMO; FARELL FOLLY

FIG.: ADOBE STOCK / KILLYKOON

Cooperations

Germany and the World

National Partners

The RI CODE is working with 68 partners in 40 cities and municipalities in Germany.

THE COOPERATION WITH other universities, public institutions and companies is part of RI CODE's self-image: We learn with and from our partners and can take the first steps towards implementing our research results in practice.

At the same time, this close exchange ensures that we understand the specific questions and problems of our partners and can consider them from a scientific perspective.

Within Germany, our network is particularly tight-knit. As part of the University of the Bundeswehr Munich, we work with 68 institutions in 40 cities and municipalities nationwide. The focus is on Bavaria and the Munich area, North Rhine-Westphalia, and Hessia. ■

	Partner	Location
1	RWTH Aachen University	Aachen
2	District of Bad Kissingen	Bad Kissingen
3	Akhetonics GmbH	Berlin
4	Berlin School of Economics and Law (HWR Berlin)	Berlin
5	Free University of Berlin (FU)	Berlin
6	German Institute for Standardisation (DIN)	Berlin
7	German National Research and Education Network (DFN)	Berlin
8	Bielefeld University of Applied Sciences and Arts (HSBI)	Bielefeld
9	IDEMIA Identity & Security Germany AG	Bochum
10	Ruhr University Bochum (RUB)	Bochum
11	Bundeswehr Centre for Digitalisation and Cyber and Information Domain Capability Development (ZDigBw)	Bonn
12	Federal Office for Information Security (BSI)	Bonn
13	Chemnitz University of Technology	Chemnitz
14	German Aerospace Center (DLR)	Cologne/Oberpfaffenhofen
15	Darmstadt University of Applied Sciences (h_da)	Darmstadt
16	Fraunhofer Institute for Computer Graphics Research (IGD)	Darmstadt
17	GSI Helmholtz Centre for Heavy Ion Research	Darmstadt
18	National Research Center for Applied Cybersecurity ATHENE	Darmstadt
19	Technical University of Darmstadt	Darmstadt
20	RapidMiner GmbH	Dortmund
21	Dresden University of Technology (TU Dresden)	Dresden
22	Helmholtz Center Dresden-Rossendorf (HZDR)	Dresden
23	State Criminal Police Office NRW (LKA NRW)	Düsseldorf
24	Friedrich-Alexander University of Erlangen-Nuremberg (FAU)	Erlangen/Nuremberg
25	Cyber Security Operations Centre of the Bundeswehr (CSOCBw)	Euskirchen
26	Frankfurt University of Applied Sciences	Frankfurt a. M.
27	nuix	Frankfurt a. M.
28	Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ)	Garching
29	Defense Technology Agency for Information Technology and Electronics (WTD 81)	Greding
30	Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)	Halle/Saale
31	Bundeswehr Command and Staff College (FüAkBw)	Hamburg
32	Helmut Schmidt University/University of the Bundeswehr Hamburg (HSU/UniBw H)	Hamburg
33	Hannover Medical School (MHH)	Hanover

	Partner	Location
34	Leibniz University Hannover (LUH)	Hanover
35	Fraunhofer Institute for Digital Media Technology (IDMT)	Ilmenau
36	Karlsruhe Institute of Technology (KIT)	Karlsruhe
37	Christian-Albrecht University of Kiel (CAU)	Kiel
38	Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw)	Koblenz
39	University of Konstanz	Konstanz
40	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
41	Otto von Guericke University Magdeburg (OVGU)	Magdeburg
42	BWI GmbH	Meckenheim
43	Bavarian State Criminal Police Office (BLKA)	Munich
44	Central Office for Information Technology in the Security Sector (ZITiS)	Munich
45	ESG Elektroniksystem- und Logistik-GmbH	Munich
46	FAST-DETECT GmbH	Munich
47	Ludwig Maximilian University Munich (LMU Munich)	Munich
48	MTU Aero Engines AG	Munich
49	Munich Police Department	Munich
50	Siemens Energy AG	Munich
51	Technical University of Munich (TUM)	Munich
52	VISTA Remote Sensing in Geosciences GmbH	Munich
53	Infineon Technologies AG	Neubiberg
54	Bavarian State Office for Information Security (LSI)	Nuremberg
55	Carl von Ossietzky University of Oldenburg	Oldenburg
56	University of Postdam (UP)	Potsdam
57	German Navy Headquarters (MarKdo)	Rostock
58	CISPA Helmholtz Center for Information Security	Saarbrücken
59	Leibniz Institute for New Materials (INM)	Saarbrücken
60	State Criminal Police Office Baden-Württemberg (LKA BW)	Stuttgart
61	Airbus Defence and Space GmbH	Taufkirchen
62	Airbus Protect GmbH	Taufkirchen
63	Hensoldt Cyber GmbH	Taufkirchen
64	Eberhard Karl University of Tübingen	Tübingen
65	Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)	Wachtberg/Bonn
66	Hessian Police Headquarters for Technology (HPT)	Wiesbaden
67	Hessian State Criminal Police Office (HLKA)	Wiesbaden
68	Federal Criminal Police Office (BKA)	Wiesbaden/Berlin


37 Kiel
Rostock 57
31
32
Hamburg
3
4
5
6
7
68
Berlin
55
Oldenburg
33
34
Hannover
56 Potsdam
8
Bielefeld
41 Magdeburg
9
10
Bochum
Dortmund
20
Halle/Saale 30
21
22
Dresden
23 Düsseldorf
13
Chemnitz
Cologne 14
11
1 Aachen
12
35 Ilmenau
25 Euskirchen
Bonn
65
Meckenheim
Wachtberg
42
38 Koblenz
26
27
Frankfurt/Main
2
Bad Kissingen
66 67 68 Wiesbaden
Darmstadt
15
16 17
18 19
Erlangen 24
Nuremberg 54
58
59
Saarbrücken
Greding 29
36
Karlsruhe
43 44
45 46
47 48
49 50
51 52
60
Stuttgart
Leinfelden-
Echterdingen
64 Tübingen
40
28
Garching
Munich
Neubiberg 53
Oberpfaffenhofen
14
Taufkirchen
61 62 63
39
Konstanz
Map legend
1 Location number of partners
Partner locations

Internationality

The RI CODE maintains a large international network. In 2024, employees came from 17 countries. We cooperated with 76 partners in 26 countries.

Employees

Nationality	Total
Argentine	1
Austrian	10
Brasilian	1
Bulgarian	1
Croatian	1
Finnish	1
French	4
Greek	2
German	111
Indic	6
Italian	2
Kosovar	1
Netherlandian	1
Polish	1
Slowenian	1
Spanish	2
South Korean	1
total	**147**

International Cooperation Partners

Country	Partner
Australia	CSIRO Data61
	Royal Melbourne Institute of Technology (RMIT)
Austria	Austrian Institute of Technology (AIT)
	Austrian Armed Forces
	Carinthia Emergency Services
	Complexity Science Hub Vienna (CSH)
	Johannes Kepler University Linz (JKU)
	Kelag-Konzern
	Municipality of Neuhaus, Carinthia
	P.SYS Caring Systems
	Software Competence Center Hagenberg
	University of Applied Sciences Campus Vienna
	Paris Lodron University of Salzburg (PLUS)
	Vienna University of Technology

FIG.: ISTOCK / BLUE PLANET STUDIO

Country	Partner
Belgium	KU Leuven
Cyprus	Centre for Social Innovation Ltd. (CSI)
Czech Republic	Center for Environmental and Technology Ethics
	Masaryk University (MU)
Denmark	Technical University of Denmark
Estonia	eu-LISA
Finland	Tampere University
France	ARIADNEXT
	Air and Space Force Academy Research Center (CREA)
	EURECOM
	Telecom SudParis
	Grenoble Alps University (UGA)
Greece	Agroknow IKE
	Athena Research and Innovation Center (ARC)
	Centre for Research and Technology Hellas (CERTH)
	EXUS Software
	Harokopio University of Athens
	IASIS NGO
	University of Athens (UoA)
	Ubitech
	University of Ioannina
	University of Piraeus
Ireland	Trilateral Research Limited Ireland (TRI-IE)
Israel	Ben-Gurion University of the Negev
Italy	Abaco S.p.A.
	Fondazione Bruno Kessler (FBK)
	University of Bologna
	University of Genoa
	University of Roma Tre
	University of Trento
	University of Turin
Japan	Kyoto University

Country	Partner
Japan	National Institute of Information and Communications Technology (NICT)
	NTT Social Informatics Laboratories
Liechtenstein	University of Liechtenstein
Luxembourg	University of Luxembourg
Netherlands	Eindhoven University of Technology (TU/e)
	University of Groningen
	University of Twente
New Zealand	University of Auckland
Norway	Norwegian University of Science and Technology (NTUT)
	University of Oslo
Poland	Wroclaw University of Science and Technology (WUST)
Serbia	Foodscale Hub
South Korea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Spain	Association Fòrum Dona Activa 2010
	Autonomous University of Madrid (UAM)
Switzerland	EPFL
	Idiap Research Institute
	University of St. Gallen (HSG)
United Kingdom	Imperial College London
	Trilateral Research Limited UK (TRI-IE)
	University of Sheffield
	University of Surrey
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	City University of New York (CUNY)
	Michigan State University
	Naval Postgraduate School (NPS)
	University of Arizona, College of Engineering

FIG.: ADOBE STOCK / ALFASMART

Young Science

Offers and Opportunities

Study Award of the Research Institute CODE 2024

Scenario analysis in the NEWSROOM project

The Research Institute CODE, together with Giesecke+Devrient GmbH, has awarded Annika S.'s thesis with the CODE Study Award 2024. In her Master's thesis, she dealt with the development of new cybersecurity scenarios and took an innovative methodological approach. The CODE Study Award was presented during the large master's ceremony on December 14, 2024, on the campus of the University of the Bundeswehr Munich.

THE INCREASE IN CYBERATTACKS on critical infrastructure or the cyberattacks in connection with the war in Ukraine are just two examples of the numerous challenges that governments and states are currently facing. At the same time, cyber security is constantly improving across Europe thanks to the regulations formulated by the European Union (EU). However, in order to achieve the goal of a uniform security level, it is also essential to promote exchange and cooperation among the European member states on all aspects of cyber security.

As part of the NEWSROOM research project funded by the European Defense Fund, systems and methods for cyber situational awareness are being developed. In this context, the aim of the thesis was to design and conduct workshops and to develop different cybersecurity scenarios in the EU based on the workshop results.

The design science approach served as the methodological framework for the development of an innovative workshop format. Based on a state-of-the-art analysis, effective, appealing workshops were designed and conducted. Attack vectors and mitigation measures were derived from the results of the workshops. As a result, the thesis presents a collection of eight different, new cybersecurity scenarios.

In her Master's thesis "Scenario analysis as part of the NEWSROOM project", Annika S. designed an innovative format that allows the development of cybersecurity scenarios in a collaborative setting. The format is adapted to the requirements of the NEWSROOM research project: It addresses the security of critical infrastructures, the military domain, attacker and defender perspectives and, above all, cooperation at European level. The format also shows where experts suspect potential threats and how difficult it is to define cooperation at a European level.

Annika S. conducted and moderated scenario workshops with international partners of the research project NEWSROOM, recorded and analyzed the results in order to eventually develop the scenarios. In her work, she entered new conceptual territory and was able to convince through creativity, competence and her skills in moderation as well as the analysis and design of the scenarios. Her Master's thesis gives new impetus to cyber security research—not only in the NEWSROOM project. ■

Prof. Geralt Siebert (l.), Prof. Karl-Heinz Renner (2.f.l.), President Eva-Maria Kern (3.f.l.) and the winners of this year's study and special awards after the ceremony.

FIG.: ADOBE STOCK / CREATIVE BRINGER; UNIVERSITY OF THE BUNDESWEHR MUNICH / SIEBOLD

Study Awards of the University of the Bundeswehr Munich

EVERY YEAR, THE University of the Bundeswehr Munich awards several study prizes donated by different partners. Since 2018, the RI CODE study award has been given to outstanding Master's graduates with a relevant thesis in the field of cyber defense. The award is funded by Giesecke+Devrient GmbH and endowed with €1,000. ■

Laureates of the last years

Year	Name	Subject of the Thesis
2018	Christian Siegert	Automated detection of vulnerabilities in IT security
2019	Philipp Sammeck	Security analysis of an electronic safe lock
2020	Robert Jurisch-Eckardt	Development of a system to fight cybercrime
2021	Martin Lukner	Synthesizing malware traces for digital forensics
2022	Lars Fuchs	Efficient exploitation of vulnerabilities in telecommunication devices
2023	Hannes Ludwig	An approach to creating adversarial samples
2024	Annika S.	Scenario analysis as part of the NEWSROOM project

Studying at the Research Institute CODE

The **Master's program** in Cyber Security at the RI CODE of the University of the Bundeswehr Munich covers information processing—including planning, formal modeling, implementation, and deployment—with a focus on technical and organizational information security. In addition to well-founded theoretical methods, practical skills are taught, e.g., such as the identification and elimination of security-relevant vulnerabilities, the development and implementation of security concepts, and the detection and mitigation of attacks on IT systems. In addition, legal and ethical issues as well as selected topics concerning the human factor in information security are covered.

The Bundeswehr supports civilian students with a **scholarship for the Master's program in Cyber Security** at the UniBw M. Requirements for this support are a degree (Bachelor or FH) in the STEM field as well as successful participation in a selection process conducted by the Assessment Center for Senior Officers of the Bundeswehr. Besides study programs at a level of excellence and an outstanding level of supervision by teaching staff, the UniBw M offers its students a wide range of leisure activities and amenities. Affordable housing options in one of Germany's most livable and diverse cities complete the benefits.

Further Information

Master's program Cyber Security:
https://go.unibw.de/mcyb
(in German)

Scholarship of the Bundeswehr:
https://go.unibw.de/stipendium-mcyb
(in German)

FIG.: CLAUS SCHUNK

DOCTORATES AND

Klement Hagenhoff

"A Framework for Controller-Based Multi-Flow Routing in MANETs"

IN MOBILE AD-HOC NETWORKS, routing and data delivery are carried out by the participants rather than by outsourced infrastructure. However, frequent node movement leads to outdated network knowledge and limited transmission capacity, making reliable data delivery challenging. Klement Hagenhoff's Ph.D. thesis explores path-finding techniques to compute stable routes while considering transmission capacity, using both adapted and new optimization concepts. Furthermore, controller-based approaches are proposed to quickly gather network topology, providing routing techniques with current connections and their characteristics.

Klement Hagenhoff received his doctorate in March 2024 under Prof. Dr. Gabi Dreo Rodosek. He currently works as an IT project coordinator at the IT Service Center of the Free State of Bavaria. ■

Julius Hermelink

"Side-Channel and Fault Attacks on Modern Lattice-Based Cryptography"

THE PROSPECT OF large-scale quantum computers threatens currently used asymmetric cryptography—Shor's algorithm could render commonly used cryptography unsafe. In his work, he presents attack strategies against lattice-based cryptography. His attack strategies combine chosen-ciphertext attacks with side-channel analysis as well as with fault attacks and target two major components of the decapsulation that process the secret key.

Moreover, he presents techniques to recover the secret key from the obtained information and shows how to combine those methods with algebraic approaches.

Julius Hermelink obtained his doctoral degree in March 2024 under the supervision of Prof. Dr. Gabi Dreo Rodosek. Currently, he is a postdoctoral researcher at the Max Planck Institute for Security and Privacy in Bochum. ■

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (1); PRIVATE (3)

HABILITATION 2024

Daniela Pöhn

"Identity Management Framework"

IN HER WORK she proposes a holistic identity management framework to improve the interoperability and security of identity management. Her framework comprises architecture, IT security, and identity management processes. The most prominent element of the architecture is the reference service model for different identity management protocols. Security proposes suitable methods, introduces new countermeasures, and offers training opportunities. The identity management processes include, e.g., cross-organizational processes depending on the applied architecture and a framework for continuous improvements.

Daniela Pöhn completed her habilitation with Prof. Wolfgang Hommel in June 2024. She is currently employed as a research assistant at the Professorship for IT Security of Software and Data. ■

Nils Rodday

"Improving Internet Routing Security: From Origin Validation to Path Validation"

THE INTERNET IS a network of networks that uses the Border Gateway Protocol (BGP) as a de-facto standard for exchanging routing information. Origin validation provides the ability to identify the correct sender of a message, while path validation allows for tracing the entire routing path. This dissertation presents new measurement methods for determining the extent of existing origin validation and develops proposals on how path validation can be best utilized as a means of enhanced security.

Nils Rodday received his PhD under Prof. Dr. Gabi Dreo Rodosek in March 2024. He is currently working as an independent IT security consultant. ■

Capture the Flag 2024

Exciting challenges at RI CODE's 10th "Capture the Flag" event

Since 2015, the "Capture the Flag" event organized by the Research Institute CODE has brought hacking enthusiasts to the University of the Bundeswehr Munich every year. Across numerous exciting challenges, participants put their skills to the test and compete with like-minded people. However, there is also plenty of fun involved. No wonder, then, that this event format has become increasingly popular and was taking place for the tenth time in 2024.

AFTER CODE CELEBRATED its tenth anniversary last year, there was yet another anniversary to celebrate this year. The "Capture the Flag" (CTF) was held for the tenth time in total, making it a fixed date in the CODE calendar. Every year in November, the event attracts numerous participants to the University of the Bundeswehr Munich campus, and this year was no exception. After a qualifying round in October, in which almost 80 teams took part, the best 24 of them received an invitation to the main round in Neubiberg.

Speed pays off

A CTF is a special cybersecurity competition in which teams compete against each other and solve various tasks—or "challenges", as they are called in CTF lingo. The time factor plays a key role, as those who solve the challenges quickly and collect the flags earn more points. If a team manages to be the first to find a solution, they receive extra points ("First Blood"). A useful bonus on the hard-fought way to the top of the scoreboard. The challenges are categorized into different types (Web Hacking, Forensic, Cryptography, Binary Exploitation, Virtual Reality etc.). To avoid boredom, the challenges are based on a different theme each year.

The theme of the CTF 2024 was based on the film "Predator", an action movie classic from 1987, in which a mercenary squad encounters a high-tech, hostile alien in the South American jungle. As in previous years, the organizers from CODE, Team localos and xo Dynamics GmbH managed to put together an event based on the plot of the film that is unmatched, at least in Munich area.

ALL FIG.: RI CODE / B. BELLGRAU

In the VR challenge, participants had to escape the Predators and solve a series of puzzles in the process.

Challenging tasks

For example, there was a virtual reality challenge in which players found themselves in a jungle where they were "hunted" by Predators. In order to escape, the first phase of the challenge involved solving a series of logic puzzles as quickly as possible and reaching a safe hideout. There, the players found a kind of Predator computer terminal, which had to be used to generate a self-destruct command for the Predators by manipulating various mechanical components. After destroying the Predators, the path through the virtual jungle could be continued and the flag found.

In another challenge from the "Cryptography" category, an encryption based on the Predator language "Yautja" had to be cracked. The characters of the Yautja alphabet consist of lines arranged at different angles around two center points per character. In addition, the key used changed with each input according to a pattern that had to be entered in the form of an initialization vector. The players were provided with an "encryption machine" that acted as a kind of "oracle" to help them solve the challenge. Once the code was cracked, an encrypted message (cipher) could be read and the flag retrieved.

Fun and competition

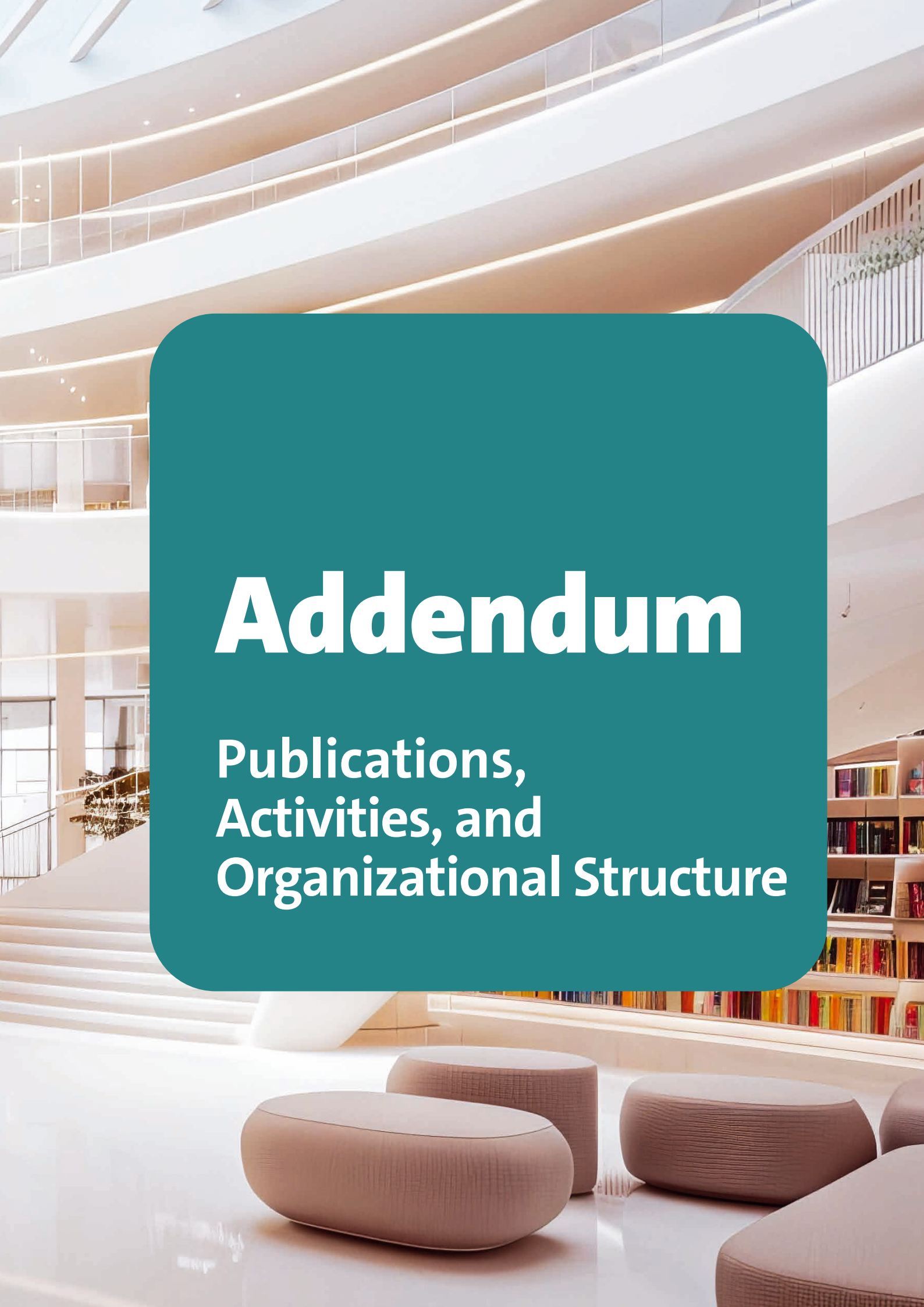
After the event started on Friday evening right on time at 6 p.m., the 24 teams from Germany and abroad fought an exciting competition throughout the night, which was extremely demanding for the participants. After a total of 18 hours, the winning team was finally announced on Saturday afternoon. With 1524 points, the "Winnie the pwnd" team came out on top, leaving the "SIGCONT" (1356 points) and "Nop(e)" teams in second and third place. At the award ceremony, CODE's Executive Director Prof. Dr. Wolfgang Hommel congratulated the three best-placed teams and presented them with their certificates. Although in the end only the winners were allowed to leave their names on the "Flag of Fame", all participants can feel like winners on this day. After all, the main focus of this type of event is on having fun and testing and developing your own skills. ■

More information:

www.unibw.de/code/events/ctf

ctf@unibw.de

FIG.: ADOBE STOCK / ADRIAN GROSU



Addendum

Publications, Activities, and Organizational Structure

Prof. Dr. Harald Baier

Digital Forensics

PUBLICATIONS

DEMMEL, M., GÖBEL, T., GONÇALVES, P., BAIER, H.: Data Synthesis is Going Mobile – On Community-driven Dataset Generation for Android Devices. Digital Threats: Research and Practice, 2024, doi: 10.1145/3688807.

DEUTSCHMANN, M., BAIER, H.: Flash-Dateisysteme im Kontext der digitalen Forensik. In: Polizei-Informatik 2024, D. Honekamp Wilfried Labudde, Ed., Remscheid: Rediroma-Verlag, 2024, pp. 115–126.

DEUTSCHMANN, M., BAIER, H.: Ubi est indicium? On forensic analysis of the UBI file system. Forensic Science International: Digital Investigation, vol. 48, no. Supplement, DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, p. 301689, 2024, [Online]. doi: 10.1016/j.fsidi.2023.301689.

GÖBEL, T., BAIER, H., TÜRR, J.: Generating Usable and Assessable Datasets Containing Anti-Forensic Traces at the Filesystem Level. In: Advances in Digital Forensics XX : 20th IFIP WG 11.9 International Conference, New Delhi, India, January 4–5, 2024, Revised Selected Papers, S. Kurkowski Elizabeth Shenoi, Ed., in IFIP Advances in Information and Communication Technology, vol. 724. Cham: Springer, 2024.

GÖBEL, T., BAIER, H., WOLF, D.: Scenario-based Data Set Generation for Use in Digital Forensics: A Case Study: 4. International Workshop on Digital Forensics (IWDF4). In: INFORMATIK 2024: Lock in or log out? Wie digitale Souveränität gelingt, Gesellschaft für Informatik e.V., Ed., in GI-Edition Lecture Notes in Informatics (LNI), vol. P352. Bonn; Berlin: Gesellschaft für Informatik, 2024, pp. 355–370. doi: 10.18420/inf2024_25.

KLIER, S., BAIER, H.: Beware of the Rabbit Hole – A Digital Forensic Case Study of DIY Drones. In: Secure IT Systems: NordSec 2024, Horn Iwaya, Leonardo; Kamm, Liina; Martucci, Leonardo; Pulls, Tobias, Ed., in Lecture Notes in Computer Science, vol. 15396. Cham: Springer, 2024, pp. 325–344. doi: 10.1007/978-3-031-79007-2_17.

KLIER, S., BAIER, H.: Scalable Image Clustering to screen for self-produced CSAM. EAI Endorsed Transactions on Internet of Things, vol. 10, pp. 1–14, 2024, doi: 10.4108/eetiot.6631.

MUNDT, M.: Die Synergie von GIS und KI. In: Polizei-Informatik 2024, D. Honekamp Wilfried Labudde, Ed., Remscheid: Rediroma-Verlag, 2024, pp. 20–29.

MUNDT, M., BAIER, H.: Adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik. Linux-Magazin, no. 2, 2024, [Online]. Available: https://www.linux-magazin.de/ausgaben/2024/02/bedrohungen-erkennen/.

MUNDT, M., BAIER, H.: Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik. In: 31. DFN-Konferenz "Sicherheit in vernetzten Systemen", DFN-Cert, Ed., Springer, 2024.

MUNDT, M., BAIER, H., RAAB-DÜSTERHÖFT, A.: Towards Reducing Business-Risk of Data Theft Implementing Automated Simulation Procedures of Evil Data Exfiltration. In: ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security, New York, NY: Association for Computing Machinery, 2024, pp. 1–12. doi: 10.1145/3664476.3664483.

RZEPKA, L., OTTMANN, J., FREILING, F., BAIER, H.: Causal Inconsistencies Are Normal in Windows Memory Dumps (too). In: Digital Threats: Research and Practice, ACM, 2024. [Online]. doi: 10.1145/3680293.

TWENNING, L., BAIER, H.: Towards arbitrating in a dispute – on responsible usage of client-side perceptual hashing against illegal content distribution. In: EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference, K. S. Li Shujun Coopamootoo, Ed., New York: Association for Computing Machinery, 2024, pp. 105–114. doi: 10.1145/3655693.3655712.

WOLF, D., GÖBEL, T., BAIER, H.: Hypervisor-based data synthesis: On its potential to tackle the curse of client-side agent remnants in forensic image generation. Forensic Science International: Digital Investigation, vol. 48, no. Supplement DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, p. 301690, 2024, doi: 10.1016/j.fsidi.2023.301690.

TEACHING

1162	**Advanced Digital Forensics**
3824	**Digital Forensics**
5001/1009	**Seminar Digital Forensics**
5501/1009	**Seminar Forensic Methods in Computer Science**
5505	**IT Forensics**

ADDITIONAL FUNCTIONS

- Reviewer for Journal of Digital Investigation and Computers & Security
- Conference Co-Chair of 13th International Conference on IT Security Incident Management & IT Forensics
- Reviewer for IFIP WG11.9 International Conference on Digital Forensics 2024
- Reviewer for DFRWS EU 2024
- Reviewer for GI Sicherheit
- Reviewer for International Conference on IT Security Incident Management & IT Forensics 2024
- Reviewer for DFRWS APAC 2024
- Reviewer for German Cybersecurity PhD Award

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

PUBLICATIONS

BERLAKOVICH, F., BRUNTHALER, S.: Cross Module Quickening – The Curious Case of C Extensions. In: Proceedings of the 38th European Conference on Object-Oriented Programming.

BERNAD, M., BRUNTHALER, S.: HOBBIT: Hashed OBject Based InTegrity. In: Proceedings of the 38th European Conference on Object-Oriented Programming.

MECHELINCK, R., DORFMEISTER, D., FISCHER, B., VOLCKAERT, S., BRUNTHALER, S.: GlueZilla: Efficient and Scalable Software to Hardware Binding using Rowhammer. In: Proceedings of the 21st Conference on Detection of Intrusions and Malware & Vulnerability Assessment.

SARAFOV, V., MARKVICA, D., BERLAKOVICH, F., BERNAD, M., BRUNTHALER, S.: Understanding and Improving Coverage Tracking with AFL++ (Registered Report). In: Proceedings of the 3rd International Fuzzing Workshop.

RESEARCH PROJECTS

APERITIF – Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

The goal is to increase the scalability of fuzzing up to datacenter scales, and subsequently perform basic research on novel parallelization and optimization of fuzzers to increase their coverage and, consequently, vulnerability yield.

Funded by: BMVg/BAAINBw
Duration: 2021–2025

DEMISEC – Detecting Malicious Implants in Source Code

Modern software depends on many external open source components written by many different parties. If the contributions of only one such party are compromised, the security of the entire product is at risk. In DEMISEC, the researchers investigate how to detect malicious source code modifications before they can subvert the development process.

Funded by: BMVg/BAAINBw
Duration: 2021–2025

DEPS – Dependable Production Environments with Software Security

The DEPS project endeavors to devise a whole family of novel techniques to protect software and intellectual property by binding software to hardware. As a result, neither will regular, known ways to attack software systems be less effective, nor will reverse en-gineering be an effective way to maliciously obtain intellectual property.

Funded by: Austrian Research Promotion Agency (FFG), Software Competence Center Hagenberg
Duration: 2022–2025

TEACHING

1009 **Seminar Language-based Security**

1009 **Seminar Optimization of Programming Languages**

1010 **Machine-oriented Programming**

3647 **Compiler Construction**

55071 **Language-based Security**

FAIRS, CONFERENCES, SEMINARS

- 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2024), Vienna, Austria (Session Chair and Panel Member at Doctoral Symposium)
- Colloquium with Prof. Dr. Shriram Krishnamurthi, Brown University, RI, USA
- 38th European Conference on Object-Oriented Programming (ECOOP 2024), Vienna, Austria
- 3rd International Fuzzing Workshop (FUZZING) 2024, Vienna, Austria
- 40th Workshop der GI-Fachgruppe Programmiersprachen und Rechenkonzepte, Bad Honnef, Germany
- DWT SWG Conference “Software Defined Defense”, Bonn, Germany

PRIZES AND AWARDS

- Distinguished Reviewer Award, IEEE SecDev 2024

ADDITIONAL FUNCTIONS

- Chair Area Board “System Security” of the Journal of Systems Research (JSYS)

Program Committee

- Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2024), Pasadena, CA, USA

Prof. Dr. Michaela Geierhos

Data Science

PUBLICATIONS

BÄUMER, F. S., SCHULTENKÄMPER, S., GEIERHOS, M., LEE, Y.S. Mirroring Privacy Risks with Digital Twins: When Pieces of Personal Data Suddenly Fit Together. SN Computer Science Vol. 5, 1109. 2024. https://doi.org/10.1007/s42979-024-03413-z.

CIMITAN, A., ALVES PINTO, A., GEIERHOS, M.: Curation of Benchmark Templates for Measuring Gender Bias in Named Entity Recognition Models. In: Calzolari, N., Kan, M.-Y., Hoste, V., Lenci, A., Sakti, S., Xue, N. (Hrsg.). Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024). ELRA and ICCL. 2024. pp. 4238–4246.

GEIERHOS, M.: Täuschend echt? Fake News! Identifikation von Desinformationskampagnen in Social Media. prmagazin Vol. 54. No. 2. Medienhaus Rommerskirchen GmbH. 2024. pp. E1–E7.

HENNEN, M., BABL, F., GEIERHOS, M.: ITER: Iterative Transformer-based Entity Recognition and Relation Extraction. In: Al-Onaizan, Y., Bansal, M., Chen, Y.-N. (Hrsg.). Findings of the Association for Computational Linguistics: EMNLP 2024. Association for Computational Linguistics. 2024. pp. 11209–11223.

MAORO, F., GEIERHOS, M.: Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen: Wie kann Künstliche Intelligenz in der Polizeiarbeit unterstützend eingesetzt werden und dabei sowohl fair als auch nachvollziehbar sein? Kongress KI@HSBI2023: Solutions im Fokus. Schriftenreihe des Institutes for Data Science Solutions 1. 2024. pp. 22–23.

MAORO, F., GEIERHOS, M.: FI CODE at GermEval 2024 GerMS-Detect closed ST1 & ST2: Ensemble- and Transformer-Based Detection of Sexism and Misogyny in German Texts. In: Krenn, B., Petrak, J., Gross, S. (Hrsg.). Proceedings of GermEval 2024 Task 1 GerMS-Detect Workshop on Sexism Detection in German Online News Fora (GerMS-Detect 2024). Association for Computational Linguistics. 2024. pp. 21–25.

MAORO, F., VEHMEYER, B., GEIERHOS, M.: Leveraging Semantic Search and LLMs for Domain-Adaptive Information Retrieval. In: Lopata, A., Gudoniene, D., Butkiene, R. (Hrsg.). Information and Software Technologies. 29th International Conference ICIST. Springer Nature Switzerland. 2024. pp.148–159.

MURAUER, J., STAUDACHER, K., GEHRKE, W., GEIERHOS, M.: Towards Masked Language Modeling in Quantum Natural Language Processing. 21st International Conference on Quantum Physics and Logic (QPL). 2024.

PRITZKAU, A., WALDMÜLLER, J., BLANC, O., GEIERHOS, M., SCHADE, U.: Current language models' poor performance on pragmatic aspects of natural language. In: Ghosh, K., Mandl, T., Majumder, P., Mitra, M. (Hrsg.). Working Notes of FIRE 2023 - Forum for Information Retrieval Evaluation (FIRE-WN 2023). 2024. pp. 159–169.

RÖSCH, P. J., OSWALD, N., GEIERHOS, M. LIBOVICKY, J.: Enhancing Conceptual Understanding in Multimodal Constrastive Learning through Hard Negative Samples. In: Gu, J., Fu, T-J., Hudson, D., Celikyilmaz, A., Wang, W. (Hrsg.). Proceedings of the 3rd Workshop on Advances in Language and Vision Research (ALVR). Association for Computational Linguistics. 2024. pp. 102–115.

SCHULTENKÄMPER, S., BÄUMER, F. S., BELLGRAU, B., LEE, Y. S., GEIERHOS, M.: From Digital Tracks to Digital Twins: On the Path to Cross-Platform Profile Linking. In: Sales, T. P., de Kinderen, S., Proper, H. A.., Pufahl, L., Karastoyanova, D., van Sinderen, M. (Hrsg.). Enterprise Design, Operations, and Computing. EDOC 2023 Workshops: IDAMS, iRESEARCH, MIDas4CS, SoEA4EE, EDOC 2023 Workshops. EDOC 2023. Lecture Notes in Business Information Processing Vol. 498. Springer Nature Switzerland. 2024. pp. 158–171.

SOARES DE SOUZA, A., MEIßNER, A., GEIERHOS, M. (2025). Combining Frequency-Based Smoothing and Salient Masking for Performant and Imperceptible Adversarial Samples. In: Antonacopoulos, A., Chaudhuri, S., Chellappa, R., Liu, CL., Bhattacharya, S., Pal, U. (eds) Pattern Recognition. ICPR 2024. Lecture Notes in Computer Science, Vol. 15322. Springer, Cham. doi: 10.1007/978-3-031-78312-8_19.

WINKEL, F., GEIERHOS, M., FINK, J.: Evaluating Embedding Models for Retrieving ESG Information from Annual Business Reports. ICIS 2024 Proceedings. Association for Information Systems (AIS). 2024.

RESEARCH PROJECTS

KIMONO – Campaign Identification, Monitoring and Classification Using Social Media Mining Methods for Integration in an AI-based Early Warning System

The aim of the KIMONO project is the detection and modeling of short- and long-term disinformation and influence campaigns in social media such as X (formerly Twitter) and Facebook. In particular, the focus is on campaigns that are driven by stately actors.

Funded by: BMVg/BAAINBw
Duration: 09/2021–12/2024

MuQuaNet – Greater Munich Quantum Internet "Authority-Dependent Risk Identification and Analysis in online Networks"

The aim is to automatically monitor selected apps and analyze the data they collect, correlate it with social media profiles, and form networks of people in order to identify potential targets and classify their risk potential on the basis of given data.

Funded by: dtec.bw
Duration: 10/2020 – 12/2026

NAWI – News Articles and Knowledge

The NAWI project deals with knowledge extraction and modeling from news articles.

Duration: 12/2021–11/2026

Synthetic Data Generation and Detection

The research project focuses on methods for generating and detecting synthetically created or manipulated data using artificial intelligence. In this context, methods are being developed that are capable of recognizing synthetically created and manipulated images, videos, and audio files accurately.

Funded by: Central Office for Information Technology in the Security Sector
Duration: 06/2022–11/2025

TACR – Technical Adaptation of Cyber Ranges for Military Use

The R&T study Technical Adaptation of Cyber Ranges for Military Use examines how the needs of Bundeswehr agencies for training facilities for the digital environment, so called cyber ranges, can be met. To this end, various use cases and cyber range products are being tested and evaluated. In addition, scenarios will be developed in a military context and tested in practice in an exercise.

Funded by: Bundeswehr Technical Center for Information Technology and Electronics in the Bundeswehr (WTD81)
Duration: 10/2023–06/2025

VIKING – Trustworthy Artificial Intelligence for Police Applications

The subproject "Explainability of Trustworthy AI Language Models for Transparent Use in Security Agencies for Text Classification" is dedicated to the research of trustworthy AI methods for text classification within the joint project VIKING.

Funded by: German Federal Ministry of Finance (BMBF)
Duration: 01/2022 – 03/2025

TEACHING

1144 Knowledge Discovery in Big Data

3850 Natural Language Processing

3851 Information Retrieval

3852 Data Science Applications

FAIRS, CONFERENCES, SEMINARS

- DeepLearn 2024, University of Maia, Portugal
- KI@BW 2024, HSU/UniBw H, Hamburg, Germany

PRIZES AND AWARDS

Study Award of the AFCEA Bonn e.V.
Hannes Jost Ludwig was awarded the first place for his Master's thesis "An Approach to Creating Adversarial Samples".

ADDITIONAL FUNCTIONS

- Faculty council member (until 09/2024)
- Member of the program committee Master's in Cyber Security
- Member of the advisory board "German Biography" of the Historical Commission at the BAdW (until 10/2024)
- Project Leader of "Deutsche Biographie" of the Historical Commission at the BAdW (since 10/2024)
- Expert for the European Commission
- Expert for VDI/VDE Innovation + Technik

Program Committee

- NAACL – Annual Conference of the North American Chapter of the Association for Computational Linguistics
- LREC-COLING 2024 – Joint International Conference on Computational Linguistics, Language Resources and Evaluation
- PATTERNS 2024 – International Conference on Pervasive Patterns and Applications
- EMNLP 2024 – Conference on Empirical Methods in Natural Language Processing
- WiNLP 2024 – Widening Natural Language Processing

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

TEACHING

10112 **Introduction to Databases**

42121 **Deep Learning**

42122 **Selected Topics in Deep Learning for IT-Security**

42111 **Biometric Recognition**

42112 **Selected Topics in Biometric Recognition**

FAIRS, CONFERENCES, SEMINARS

- IEEE Int. Conference of the Biometrics Special Interest Group (BIOSIG) – General Chair
- IEEE Int. Joint Conference on Biometrics (IJCB) – Program Co-Chair
- IEEE Int. Workshop on Biometrics and Forensics (WIFS) – Special Session Chair Co-Chair

ADDITIONAL FUNCTIONS

- General Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG)
- Chair of the BIOSIG special interest group of the Gesellschaft für Informatik (GI)
- Deputy Chair of the European Association for Biometrics (EAB)
- Member of the IARP TC4 Conference Committee, the IEEE Biometrics Council Security and Privacy Technical Committee, and the IEEE Information and Forensics Technical Committee
- Delegate of the German Institute for Standardisation (DIN) in ISO/IEC SC37 JTC1 SC37 on biometrics
- Co-Affiliation Norwegian University of Science and Technology (NTNU)

Prof. Dr. Wolfgang Hommel

Software and Data Security

PUBLICATIONS

BIERWIRTH, T., PFÜTZNER, S., SCHOPP, MA., STEININGER, C.: Design and Evaluation of Advanced Persistent Threat Scenarios for Cyber Ranges. IEEE Access. Vol. 12. 2024. pp. 72458-72472.

FRANK, A., STEINKE, M., HOMMEL, W.: Lowcaf: A Low-Code Protocol Analysis Framework. In: 20th International Conference on Network and Service Management (CNSM). Prague, Czech Republic: IFIP, IEEE, 2024.

FRIES, I., GRABATIN, M., HOFMEIER, M.: Sovereign by Design: The LIONS Approach to Digital Sovereignty. Logos Verlag Berlin, 2024 – ISBN 978-3-8325-5834-5.

GEISLER, M., PÖHN, D., HOMMEL, W.: Hooked: A Real-World Study on QR Code Phishing. DFN-Konferenz Sicherheit in vernetzten Systemen (31., 2024, Hamburg). 2024.

HOFMEIER, M., GRABATIN, M., HOMMEL, W.: System Design for Electronic Signatures within Supply Chains using Blockchain Technology and Self-Sovereign Identities. In: Sovereign by Design: The LIONS Approach to Digital Sovereignty (2024), pp. 143–160.

HOFMEIER, M., PÖHN, D., HOMMEL, W.: DistIN: Analysis and Validation of a Concept and Protocol for Distributed Identity Information Networks. ARES ,24: Proceedings of the 19th International Conference on Availability, Reliability and Security. New York, NY, USA. Association for Computing Machinery. 2024.

LESCHKE, N., PÖHN, D., PALLAS, F.: How to Drill into Silos: Creating a Free-to-Use Dataset of Data Subject Access Packages. In: Jensen, Meiko; Laurasoux, Cédric; Rannenberg, Kai (Ed.). Privacy Technologies and Policy. 12th Annual Privacy Forum, APF 2024, Karlstad, Sweden, September 4–5, 2024, Proceedings. Cham. Springer. 2024.

MAUL, D., STIEMERT, L., PÖHN, D.: Evaluation of Basic Methods to Bypass Recent Antivirus Systems in Windows Environments. DFN-Konferenz Sicherheit in vernetzten Systemen (31., 2024, Hamburg). 2024.

PÖHN, D., GRABATIN, M., HOMMEL, W.: Analyzing the Threats to Blockchain-Based Self-Sovereign Identities by Conducting a Literature Survey. Applied Sciences. Vol. 14. 2024. No. 1.

PÖHN, D., GRUSCHKA, N.: Past and Present: A Case Study of Twitter's Responses to GDPR Data Requests. In: Rannenberg, Kai; Drogkaris, Prokopios; Lauradoux, Cédric (Ed.). Privacy Technologies and Policy. 11th Annual Privacy Forum, APF 2023, Lyon, France, June 1–2, 2023, Proceedings. Cham. Springer. 2024. pp. 57-84. Lecture Notes in Computer Science.

PÖHN, D., HOMMEL, W.: Digital Skills and Technology to Empower Women. In: Krishnan, Saravanan; Anand, A. Jose; Kumar, Raghvendra (Ed.). Sustainable Development Goals. Technologies and Opportunities. Boca Raton. CRC Press. 2024.

RESEARCH PROJECTS

6G-life

The 6G-life project uses a holistic approach to research innovative concepts in the field of scalable communication, new methods, flexible software concepts and adaptive hardware that support the basic idea of human-machine collaboration. In all research fields, the requirements for latency, resilience, security and sustainability are always addressed in parallel as multidisciplinary topics.

Funded by: German Federal Ministry of Finance (BMBF) (subcontracted by TU Munich)
Duration: 12/2022 – 08/2025

ACSE LTE – Airborne Cybersecurity Enhancement Long Term Evolution

Airborne Cybersecurity Enhancement (ACSE) LTE (Long Term Evolution) is the successor to the ACSE project that concluded at end of 2023. As its predecessor, ACSE LTE is a research cooperation between FI CODE and Airbus Defence and Space. The focus of this project is the application of insights gained during the previous project regarding secure aircraft communication to tactical data links.

Funded by: Airbus Defence and Space
Duration: 01/2024–12/2025

Application-Oriented Technology Potential for Cyber/IT

The goal of the R&T measure "Application-oriented technology potential for cyber/IT" is to identify research ideas and innovations, to bring together diverging interests, goals, and methods in the area of cybersecurity and cyberdefense research, and to promote cross-sector cooperation in the area of technology monitoring in cybersecurity.

Funded by: WTD 81
Duration: 07/2024–12/2026

DEFINE – DC-Grids for Reliable Power Supply

Modern power grids are fed from renewable power sources such as solar or wind energy and serve increasingly demanding needs such as electromobility. Direct current distribution grids promise an advantage over conventional AC grids regarding efficiency and control. RI CODE is researching hardened IT and suitable monitoring just as control solutions for these future energy supply grids.

Funded by: dtec.bw
Duration: 01/2021–12/2026

Ledger Innovation and Operation Network for Sovereignty (LIONS)

The LIONS project builds a research platform for enhancing the resilience and digital sovereignty of digitalization using distributed ledger technologies. As part of the inter-disciplinary research project, the research group focuses on the topic of self-sovereign identity management and the technical support of project partners.

Funded by: dtec.bw
Duration: 01/2021–12/2026

ROLORAN – Resilient Operation of LoRa Networks

As a long-range, energy-efficient radio technology, LoRaWAN offers a promising basis for stable long-range communication. This project investigates the robustness and limits of LoRaWAN through experimental and theoretical analyses, supports protocol security through software hardening and demonstrates the applicability by developing selected prototypes and setting up exemplary IoT infrastructures.

Funded by: dtec.bw
Duration: 01/2021–12/2026

TACR – Technical Adaptation of Cyber Ranges for Military Use

The R&T study Technical Adaptation of Cyber Ranges for Military Use examines how the needs of Bundeswehr agencies for training facilities for the digital environment, so-called cyber ranges, can be met. To this end, various use cases and cyber range products are being tested and evaluated. In addition, scenarios will be developed in a military context and tested in practice in an exercise.

Funded by: Bundeswehr Technical Center for Information Technology and Electronics in the Bundeswehr (WTD81)
Duration: 10/2023–06/2025

TEACHING

1006 **Introduction to Computer Science 1**

1007 **Introduction to Computer Science 2**

3459 **Selected Chapters of IT Security**

5501 **Seminar Application and Software Security**

5501 **Seminar Information Security Management**

5507 **Secure Networked Applications**

5508 **Information Security Management**

FAIRS, CONFERENCES, SEMINARS

- Workshop Chair EDId @ ARES 2024 (Dr. Daniela Pöhn)

PRIZES AND AWARDS

- ITIS e.V. Research Award for Dr. Michael Grabatin and his dissertation "Architecture and Tools for Self-sovereign Identity Management on Distributed Ledgers"

ADDITIONAL FUNCTIONS

- Dean of the Computer Science department
- Board of Examiners for Master of Intelligence & Security Studies
- Member of the Operating Committee of the German Research and Education Network
- Expert in the research funding program "Sparkling Science 2.0"

Program Committee

- IEEE/IFIP International Symposium on Integrated Network Management
- IEEE/IFIP Network Operations and Management Symposium
- IEEE International Conference on Communications
- DFN Conference Security in Networked Systems
- Workshop on Avionics Systems and Software Engineering
- International Workshop on Frontiers in Availability, Reliability and Security
- International Journal of Critical Infrastructure Protection
- International Journal of Electronic Government
- International Journal of Innovation and Technology Management

Prof. Dr. Ulrike Lechner

Information Systems Research Group

PUBLICATIONS

BECHARA, J., LECHNER, U. (2024). Digital sovereignty and open-source software–A discussion paper. In: International Conference on Innovations for Community Services (pp. 397–407). Springer Nature Switzerland Cham.

ESPINHA GASIBA, T., IOSIF, A.-C., KESSBA, I., AMBURI, S., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). May the source be with you: On ChatGPT, cybersecurity, and secure coding. Information, 15(9), 572.

FAHRNBERGER, G., SCHAUER, S., LECHNER, U. (2024). Check for scared? Prepared? Toward a ransomware incident response scenario 9. In: Innovations for Community Services: 24th International Conference, I4CS 2024, Maastricht, The Netherlands, June 12–14, 2024, Proceedings (Vol. 2109, p. 289). Springer Nature.

FRIES, I., GRABATIN, M., HOFMEIER, M. (eds.) (2024). Sovereign by Design. The LIONS Approach to Digital Sovereignty. Logos Verlag Berlin.

GREINER, M., SEIDENFAD, K., LANGEWISCH, C., HOFMANN, A., LECHNER, U. (2024). The digital product passport: Enabling interoperable information flows through blockchain consortia for sustainability. In: International Conference on Innovations for Community Services (pp. 377–396). Springer Nature Switzerland Cham.

GREINER, M., STRUSSENBERG, J., SEILER, A., HOFBAUER, S., SCHUSTER, M., STANO, D., FAHRNBERGER, G., SCHAUER, S., LECHNER, U. (2024). Scared? Prepared? Toward a ransomware incident response scenario. In: International Conference on Innovations for Community Services (pp. 289–320). Springer Nature Switzerland Cham.

GREINER, M., ZEISS, C., NEIS, N., SEIDENFAD, K., LECHNER, U., WINKELMANN, A. (2024). Governance Requirements for Decentralized Blockchain-based Supply Chain Consortia. Wirtschaftsinformatik 2024 Proceedings. 58. https://aisel.aisnet.org/wi2024/58

IOSIF, A.-C., ESPINHA GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). To kill a mocking bug: Open source repo mining of security patches for programming education. In: 5th International Computer Programming Education Conference (ICPEC 2024) (pp. 16:1–16:12). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

IOSIF, A. C., LECHNER, U., PINTO-ALBUQUERQUE, M., ESPINHA GASIBA, T. (2024). Code review for cybersecurity in the industry: Insights from gameplay analytics. In: 5th International Computer Programming Education Conference (ICPEC 2024) (pp. 1–11). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

IOSIF, A.-C., LECHNER, U., PINTO-ALBUQUERQUE, M., ESPINHA GASIBA, T. (2024). Cybersecurity awareness training for industrial software developers via a serious game for code review.

IOSIF, A.-C., LECHNER, U., PINTO-ALBUQUERQUE, M., GASIBA, T. E. (2024). Serious game for industrial cybersecurity: Experiential learning through code review. In: 2024 36th International Conference on Software Engineering Education and Training (CSEE&T) (pp. 1–6). IEEE.

KLARE, M., LECHNER, U. (2024). A reference model to strengthen digital sovereignty in companies. The 15th International Conference on Software Business (ICSOB 2024), November 18–20, 204, Utrecht, the Netherlands.

LIONS Monitor. Individuals Perspectives on Information Technology and E-Signatures. Universität der Bundeswehr München, 2024.

MÜLLER, K., KOLB, L., LECHNER, U., BODENDORF, F. (2024). Ethical AI principles for enterprise collaboration in federated learning networks.

REINHARD, P., NEIS, N., KOLB, L., WISCHER, D., LI, M. M., WINKELMANN, A., TEUTEBERG, F., LECHNER, U., LEIMEISTER, J. M. (2024). Augmenting frontline service employee onboarding via hybrid intelligence: Examining the effects of different degrees of human-GenAI interaction. In: International Conference on Design Science Research in Information Systems and Technology (pp. 384–397).

REINHARD, P., NEIS, N., KOLB, L., WISCHER, D., WINKELMANN, A., TEUTEBERG, F., LECHNER, U. (2024). Check for updates: Augmenting frontline service employee onboarding via hybrid intelligence: Examining the effects of different degrees. In: Design Science Research for a Resilient Future: 19th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2024, Trollhättan, Sweden, June 3–5, 2024, Proceedings (Vol. 14621, p. 384). Springer Nature.

SEIDENFAD, K., GREINER, M., BIERMANN, J., DANNENBERG, D., KEINEKE, S., LECHNER, U. (2024). Check for greenhouse gas emissions as commons: A community service approach with blockchain on the edge. In: Innovations for Community Services: 24th International Conference, I4CS 2024, Maastricht, The Netherlands, June 12–14, 2024, Proceedings (Vol. 2109, p. 351). Springer Nature.

SEIDENFAD, K., GREINER, M., BIERMANN, J., DANNENBERG, D., KEINEKE, S., LECHNER, U. (2024). Greenhouse gas emissions as commons: A community service approach with blockchain on the edge. In: International Conference on Innovations for Community Services (pp. 351–376). Springer Nature Switzerland Cham.

SEIDENFAD, K., GREINER, M., BIERMANN, J., LECHNER, U. (2024). Blockchain-based monitoring, reporting and verification of GHG emissions on the network edge–a system integration study in the artisan coffee industry. In 2024 IEEE/SICE International Symposium on System Integration (SII) (pp. 1227–1228).

SEILER, A., LECHNER, U., STRUSSENBERG, J., HOFBAUER, S. (2024). Operation Raven: Design of a cyber security incident response game. In: International Conference on Innovations for Community Services (pp. 337–347). Springer Nature Switzerland Cham.

WURZENBERGER, M., KRENN, S., LANDAUER, M., SKOPIK, F., PERNER, C., LÖTJÖNEN, J., PÄIJÄNEN, J., GARDIKIS, G., ALABASIS, N., SAKERMAN, L., et al. (2024). NEWSROOM: Towards automating cyber situational awareness processes and tools for cyber defence. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1–11).

ZHAO, T., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. Journal of Systems and Software, 210, 111946.

ZHAO, T., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M., ONGU, D. (2024). COPYCAT: Applying serious games in industry for defending supply chain attack. In: International Conference on Innovations for Community Services (pp. 321–336). Springer Nature Switzerland Cham.

ZHAO, T., ONGU, D., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). A deep dive into CATS evaluator algorithm: Quantification of the probability in serious game cloud security defense scenarios. In: 2024 36th International Conference on Software Engineering Education and Training (CSEE&T) (pp. 1–5). IEEE.

RESEARCH PROJECTS

LIONS – Ledger Innovation and Operation Network for Sovereignty

The interdisciplinary research project is developing a platform for investigating distributed ledger technology as a digitalization technology to increase resilience and digital sovereignty. This includes the further development of distributed and sovereign identity management under security and protection aspects in application areas such as IoT, web applications and eGovernance.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.
Duration: 01/2021–12/2026

FAIRS, CONFERENCES, SEMINARS

LIONS Symposium on November 05 2024, at the University of the Bundeswehr Munich: https://www.unibw.de/lions/symposium

Prof. Dr.-Ing. Mark Manulis

Privacy and Applied Cryptography Lab

PUBLICATIONS

LI, N., LI, Y., MANULIS, M., TIAN, Y., YANG, G.: Practical and secure policy-based chameleon hash for redactable blockchains. The Computer Journal 2024.

MANULIS, M., NGUYEN, J.: Fully Homomorphic Encryption beyond IND-CCA1 Security: Integrity through Verifiability. EUROCRYPT 2024.

MENG, L., CHEN, L., TIAN, Y., MANULIS, M.: FABESA: Fast (and Anonymous) Attribute-Based Encryption under Standard Assumption. ACM CCS 2024.

MENG, L., CHEN, L., TIAN, Y., MANULIS, M., LIU, S.: FEASE: Fast and Expressive Asymmetric Searchable Encryption. USENIX Security Symposium 2024.

RESEARCH PROJECTS

LIONS – Ledger Innovation and Operation Network for Sovereignty

The interdisciplinary research project is developing a platform for investigating distributed ledger technology as a digitalization technology to increase resilience and digital sovereignty. This includes the further development of distributed and sovereign identity management under security and protection aspects in application areas such as IoT, web applications and eGovernance.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.
Duration: 01/2025–12/2026

PiQASO – Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

The aim is to provide optimized crypto services for key encapsulation, signatures, key exchange, authorization, identity management and secure computation. The goal is to provide a public key infrastructure that is robust against quantum computer attacks and can be integrated without special hardware. This will enable quantum-safe encryption services for existing systems.

Funded by: EU Horizon Europe
Duration: 01/2025–12/2027

SECANT – Security and Privacy Protection in Internet of Things Devices

The project is developing an innovative cybersecurity risk assessment platform to address cascading cyber threats and increase privacy and data protection across the connected ICT ecosystem. PACY Lab is working on cryptographic protocols based on blockchain technology to enable privacy-preserving search over encrypted sensitive data.

Funded by: EU H2020
Duration: 09/2021–08/2024
Participation via University of Surrey, UK

TEACHING

55481 **Modern Cryptography**

55482 **Research Trends in Cryptography**

55631 **Private Data Processing**

55632 **Private Authentication and Messaging**

55633 **Seminar Privacy Enhancing Cryptography in Practice**

ADDITIONAL FUNCTIONS

- Associate Editor of IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor of International Journal of Information Security (IJIS), Springer
- Visiting professor at the University of Surrey, UK

Program Committee

- 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2024), Zurich, Switzerland

Jun. Prof. Dr. Maximilian Moll

Operations Research — Prescriptive Analytics

PUBLICATIONS

MILANI, R., MOLL, M., DE LEONE, R.(2024). Detection of Important States through an Iterative Q-value Algorithm for Explainable Reinforcement Learning. Proceedings of the 57th Hawaii International Conference on System Sciences, pp. 1401–1408.

PHAM, T. S., NISTOR, M. S., CAO, L., GERSCHBERGER, M., MOLL, M. (2024). Machine Learning in Vehicle Travel Time Estimation: A Brief Technological Perspective and Review. Proceedings of the 57th Hawaii International Conference on System Sciences, pp. 1409–1414.

RESEARCH PROJECTS

Digital Workplace and Human AI-Assisted Training Through Touch

Considering the importance of artificial assistance systems, the project investigates their inclusion in the training process. This is done from the perspective of human learning (cognitive science), machine learning (computer science) and by analyzing trust in AI partners (philosophy).

Funded by: Bavarian Research Institute for Digital Transformation (bidt)
Duration: 04/2022–03/2024

TEACHING

10361 **Operations Research**

14901 **Selected Chapters of Operations Research and Decision Theory**

29941 **Selected Chapters of Data-driven Optimization**

22942 **Quantum Machine Learning & Optimization**

3396 **Data Mining**

ADDITIONAL FUNCTIONS

- Fellow of the Bavarian Science Alliance for Peace, Conflict and Security Research
- Coordinator of the program for highly talented students at the University of the Federal Armed Forces Munich
- Working Group Leader of "Simulation and Optimization of Complex Systems", German Operations Research Society

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLICATIONS

ALVAREZ, J. M., COLMENAREJO, A. B., ELOBAID, A., FABBRIZZI, S., FAHIMI, M., FERRARA, A., GHODSI, S., MOUGAN, C., PAPAGEORGIOU, I., REYERO, P., et al. (2024). Policy advice and best practices on bias and fairness in AI. Ethics and Information Technology, 26(2):31.

GHODSI, S., SEYEDI, S. A., NTOUTSI, E. (2024). Towards cohesion-fairness harmony: Contrastive regularization in individual fair graph clustering. In_ Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), pp. 284–296. Springer.

HUUK, J., DHINGRA, A., NTOUTSI, E., DENKENA, B. (2024). Shape error prediction in 5-axis machining using graph neural networks. In: 18th CIRP ICME Conference on Intelligent Computation in Manufacturing Engineering.

KUMAR, V., NTOUTSI, E., RAJAWAT, P. S., MEDDA, G., RECUPERO, D. R. (2024). Unlocking LLMs: Addressing scarce data and bias challenges in mental health. In: 1st International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security (NL-PAICS).

PANAGIOTOU, E., HEURICH, M., LANDGRAF, T., NTOUTSI, E. (2024a). TABCF: Counterfactual explanations for tabular data using a transformer-based VAE. In Proceedings of the 5th ACM International Conference on AI in Finance (ICAIF), pp. 274–282.

PANAGIOTOU, E., ROY, A., NTOUTSI, E. (2024b). Synthetic tabular data generation for class imbalance and fairness: A comparative study. In: BIAS Workshop co-located with ECML PKDD 2024.

QIAN, H., PANAGIOTOU, E., PENG, M., NTOUTSI, E., KANG, C., MARX, S. (2024). A novel dataset and feature selection for data-driven conceptual design of offshore jacket substructures. Ocean Engineering, 303:117679.

RAMANAIK, C. K., ROY, A., NTOUTSI, E. (2024a). Adversarial robustness of vaes across intersectional subgroups. In: BIAS Workshop co-located with ECML PKDD 2024.

RAMANAIK, C. K., WILLMANN, A., SUAREZ CARDONA, J.- E., HANFELD, P., HOFFMANN, N., HECHT, M. (2024b). Ensuring topological data-structure preservation under autoencoder compression due to latent space regularization in Gauss-Legendre nodes. Axioms, 13(8):535.

ROY, A., KOUTLIS, C., PAPADOPOULOS, S., NTOUTSI, E. (2024). Fairbranch: Mitigating bias transfer in fair multi-task learning. In: 2024 International Joint Conference on Neural Networks (IJCNN), pp. 1–8. IEEE.

SWATI, S. MLADENÍC, D. (2024). LLNewsBias: A multilingual news dataset for lifelong learning. In: Proceedings of the 27th International Multiconference Information Society (IS) 2024, volume C, pp. 97–100.

SWATI, S., ROY, A., NTOUTSI, E. (2024). Exploring Fusion Techniques in Multimodal AI-Based Recruitment: Insights from FairCVdb. In: Third European Workshop on Algorithmic Fairness (EWAF).

RESEARCH PROJECTS

Hephaestus – Machine Learning Methods for Adaptive Process Planning of 5-Axis Milling

The project aims to research a framework for a learning 5-axes compensation of shape errors in milling processes based on a process-parallel material removal simulation and sophisticated machine learning (ML) strategies. Moreover, we aim to investigate the ability of knowledge transfer between different workpiece geometries, milling tools and machine tools for an enhanced process planning.

Funded by: DFG
Duration: 04/2021–05/ 2025

MAMMoth –Multi-Attribute, Multimodal Bias Mitigation in AI Systems

MAMMoth concentrates on identifying and addressing (multi-)discrimination in AI systems concerning various protected attributes, encompassing both conventional tabular data and more intricate network and visual data. The developed solutions will be pilot tested in three relevant sectors of interest: a) finance/loan applications, b) identity verification systems, and c) academic evaluation.

Funded by: EU
Duration: 09/2022–08/2025

STELAR – Spatio-Temporal Linked Data Tools for the Agri-Food Data Space

STELAR will design, develop, evaluate, and showcase an innovative Knowledge Lake Management System (KLMS) to support and facilitate a holistic approach for FAIR (Findable, Accessible, Interoperable, Reusable) and AI-ready (high-quality, reliably labeled) data that will be pilot tested in diverse, real-world use cases in the agrifood data space.

Funded by: EU
Duration: 09/2022–08/2025

TEACHING

2319 **Artificial Intelligence (WT)**

2320 **Responsible Artificial Intelligence (HT)**

2534 **Machine Learning (FT)**

FAIRS, CONFERENCES, SEMINARS

- European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2024)(Program Co-Chair)
- 1st Workshop on Responsible AI, co-located with Hellenic Conference on Artificial Intelligence (SETN)(Co-Organizer)
- European Summer School on Artificial Intelligence (ESSAI) – Course on Fairness and Explainability: Models, Measurements and Mitigation Strategies
- AI@LMU lecture series – Guest lecture on AI bias and fairness
- INDOR lecture sereis "Maschinen wie wir", UniBwM – Invited talk: Bias in AI and why we should care?
- 2nd EMERGENCY-VRD workshop on Moral and Legal Aspects of Autonomous Systems, UniBwM – Invited talk: Technical aspects of autonomous systems
- Workshop on fostering a fair algorithmic environment: Presenting the MAMMOth AI bias solutions, Complexity Science Hub, Vienna – Invited talk: The multifaced nature of bias in AI
- Workshop on unmasking biases in data collection, University of Toronto (online) – Invited talk: Bias and discrimination in AI systems
- Panel on Weaving An Ethical and Human-Centric Web, International Conference on Web Engineering (ICWE), Tampere, Finland
- Panel discussion: AI vs Human at Versus Festival, Austria
- Summer workshop on KI in Aktion: Chancen und Grenzen lernfähiger Maschinen, UniBw M

ADDITIONAL FUNCTIONS

- Member of the program committee Master's in Cyber Security
- Faculty representative for the Fakultätentag Informatik (FTI)
- Expert for the European Commission
- Expert for the Luxembourg National Research Fund
- Expert for the Swedish Research Council
- External advisory board member for the EU project ExtremeXP
- Co-Affiliation L3S Research Center, Hannover.

Program Committee

- International Joint Conference on Artificial Intelligence (IJCAI)
- ACM Conference on Fairness, Accountability, and Transparency (FAccT)

Prof. Dr. Stefan Pickl

Operations Research — Research Group COMTESSA

TEACHING

10245 **Operations Research Lab – Decision Support**

10252 **Seminar Operations Research I**

10371 **Introduction to Business Information Systems**

10372 **Principles of Information and Communication Technology**

10401/2 **Introduction to Business Intelligence**

12311 **Data Mining and IT-based Decision Support**

12325 **Operations Research Lab – Decision Support II**

12326 **Selected Chapters of Operations Research Seminar II**

2038-V1 **AI and Data-driven Optimization**

3481-V1 **Data Science and Analytics**

ICE Lecture 2024

Lecture at the Intelligence College in Europe together with Gehard Conrad and Maximilian Moll: "Cyber and its Implications for Intelligence, Analysis and Decision Making"

ADDITIONAL FUNCTIONS

- Vice-President German Committee on Disaster Prevention
- Chair of the Advisory Board German Operations Research Society
- Member of the DEU NATO SAS Panel
- Member of Munich Aerospace
- Member of the Board of Trustees Hessian Academy of Highly Gifted Pupils
- Steering Committee Member of VOICE – National Society of IT-Users
- Member of the German Academy of Technology ACATECH

Prof. Dr. Daniel Slamanig

Cryptology

PUBLICATIONS

ABDOLMALEKI, B., GLAESER, N., RAMACHER, S., SLAMANIG, D.: Circuit-Succinct Universally-Composable NIZKs with Updatable CRS. 37th IEEE Computer Security Foundations Symposium, CSF 2024, Enschede, Netherlands, July 8–12, 2024, IEEE Computer Society Digital Library.

CAPUANO, L., MULA, M., TERRACINI, L.: Quarternionic p-adic continued fractions. Communications in Algebra, 2024, Taylor & Francis.

CELI, S., GRIFFY, S., HANZLIK, L., PEREZ KEMPNER, O., SLAMANIG, D.: SoK: Signatures with Randomizable Keys. 28th International Conference on Financial Cryptography and Data Security – FC 2024.

CINI, V., RAMACHER, S., SLAMANIG, D., STRIECKS, C., TAIRI, E.: (Inner-Product) Functional Encryption with Updatable Ciphertexts. Journal of Cryptology, 37, 8, 2024, Springer.

DERLER, D., SAMELIN, K., SLAMANIG, D.: Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes. Journal of Cryptology, 37, 29, 2024, Springer.

GARCÍA-RODRÍGUEZ, J., KRENN, S., SLAMANIG, D.: To Pass or Not to Pass: Privacy-Preserving Physical Access Control. In: Computers & Security, 2024, Elsevier.

GRIFFY, S., LYSYANSKAYA, A., MIR, O., PEREZ KEMPNER, O., SLAMANIG, D.: Delegatable Anonymous Credentials from Mercurial Signatures With Stronger Privacy. 30th Annual International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2024.

MITROKOTSA, K., MUKHERJEE, S., SEDAGHAT, M., SLAMANIG, D., TOMY, J.: Threshold Structure-Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. 27th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2024.

MULA, M., MURRU, N., PINTORE, F.: On Random Sampling of Supersingular Elliptic Curves. Annali di Matematica Pura ed Applicata (1923 -), 2024, Springer.

SKOPIK, F., BONITZ, A., SLAMANIG, D., KIRSCHNER, M., HACKER, W.: Towards a single device for multiple security domains. Journal of Universal Computer Science 30(5): 563-589.

TEACHING

10251 **Seminar Cryptology (Master)**

39311 **Introduction to Post-Quantum Cryptography**

55011 **Seminar Cryptology (Bachelor)**

FAIRS, CONFERENCES, SEMINARS

- 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2024), Zürich
- Workshop on Foundations and Applications of Zero-Knowledge Proofs, Edinburgh
- Leuven Isogeny Days 5, Leuven
- Leuven I-sage-ny Days, Leuven
- Cifris 24 Workshop on Number Theory and Cryptography (NTC24), Rome
- QSI PQC Spring School 2024, Porto
- Math PQC Conference, Budapest
- Young Researcher Crypto Seminar Spring 2024, Paderborn

ADDITIONAL FUNCTIONS

- Reviewer for the European Commission
- Reviewer for the Deutsche Forschungsgemeinschaft (DFG)
- Academic Editor for IET Information Security
- Editor for the Journal of Universal Computer Science
- Keynote Speaker at the 19th IFIP Summer School on Privacy and Identity Management 2024
- Invited Speaker at the "AB+ – Attributes and Blindness" workshop co-located with EUROCRYPT 2024
- Participation in the Panel "Cyber Security", Technologie- und Innovationsforum Salzburg (salz21), Salzburg

Program Committee

- 44th Annual International Cryptology Conference (CRYPTO 2024)
- 31st Annual ACM Conference on Computer and Communications Security (ACM CCS 2024)
- 22nd International Conference on Applied Cryptography and Network Security (ACNS 2024)
- 30th Australasian Conference on Information Security and Privacy (ACISP 2024)
- 39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024)
- 18th International Conference on Provable and Practical Security (ProvSec 2024)
- 19th International Workshop on Security (IWSEC 2024)
- 11th ACM Asia Public-Key Cryptography Workshop (APKC 2024)
- 24th Central European Conference on Cryptology (CECC 2024)

Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

TEACHING

1016 **Introduction to Operating Systems**

1026 **Distributed Systems**

1031 **Virtualization**

5505 **Operating Systems Security**

ADDITIONAL FUNCTIONS

- Member of the examinations board for Master Cybersecurity
- Member of the study program commission for Master Cybersecurity
- Member of the examinations board for Computer Science
- Member of the examinations board for Information Systems

Prof. Dr. Arno Wacker

Privacy and Compliance

PUBLICATIONS

KLEINE, S., MÜLLER, K.: On the growth of the Jacobians in $\mathbb{Z}_p^l$-voltage covers of graphs, Algebraic Combinatorics, Volume 7 (2024) no. 4, pp. 1011–1038. doi: 10.5802/alco.366.

SCHLOLAUT, M., KIESELMANN, O., WACKER, A.: Comparing Nudges and Deceptive Patterns at a Technical Level. 2024 Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024), Honolulu, HI, USA. https://ceur-ws.org/Vol-3720/paper12.pdf.

TEACHING

3480 **Secure Networks and Protocols**

55011 **Vulnerabilities and Attack Vectors Seminar**

55041 **Data Privacy**

55042 **Privacy Enhancing Technologies**

55061 **Introduction to Cryptography**

55062 **Kryptoanalyse**

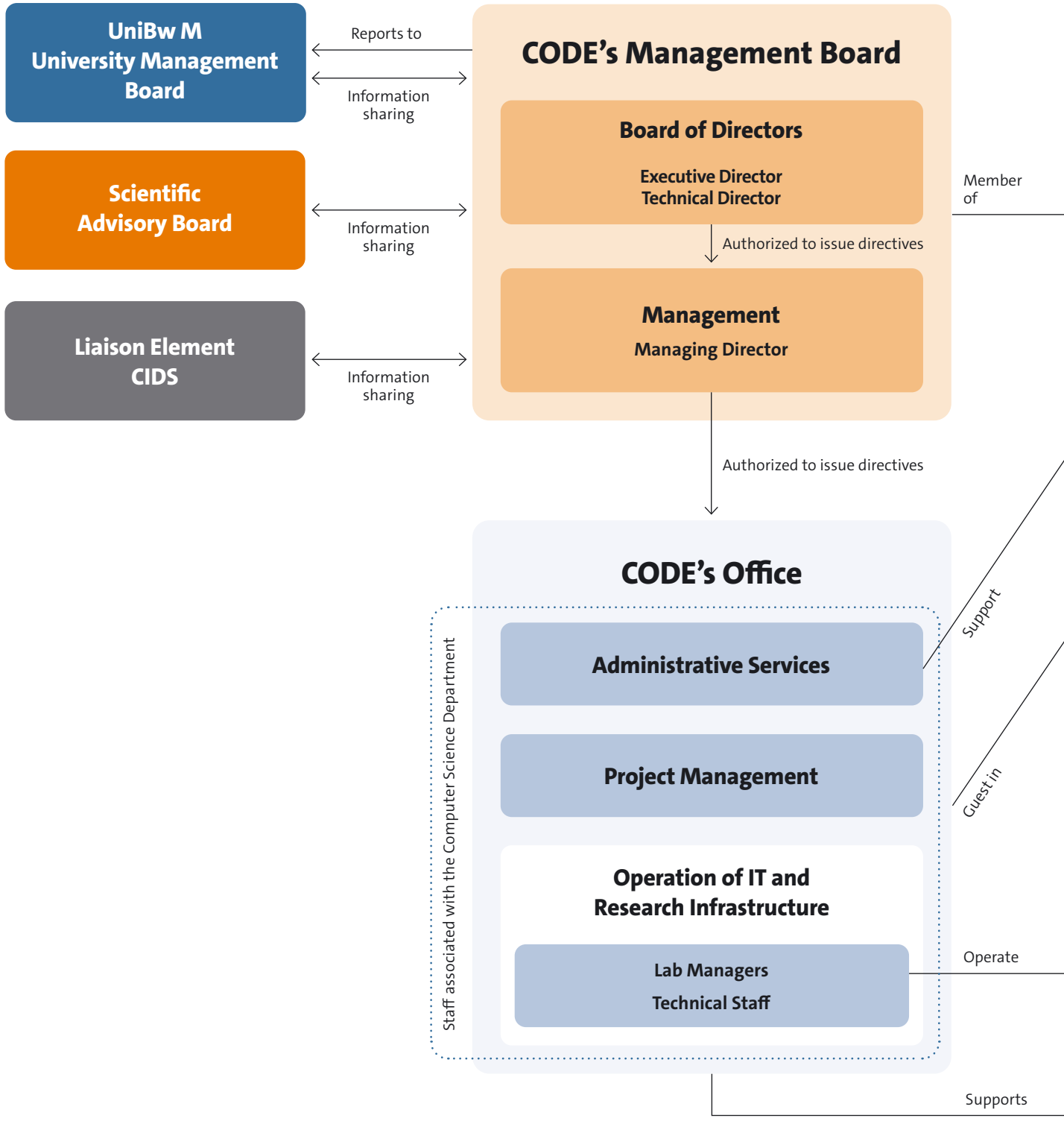
55091 **Penetration Testing**

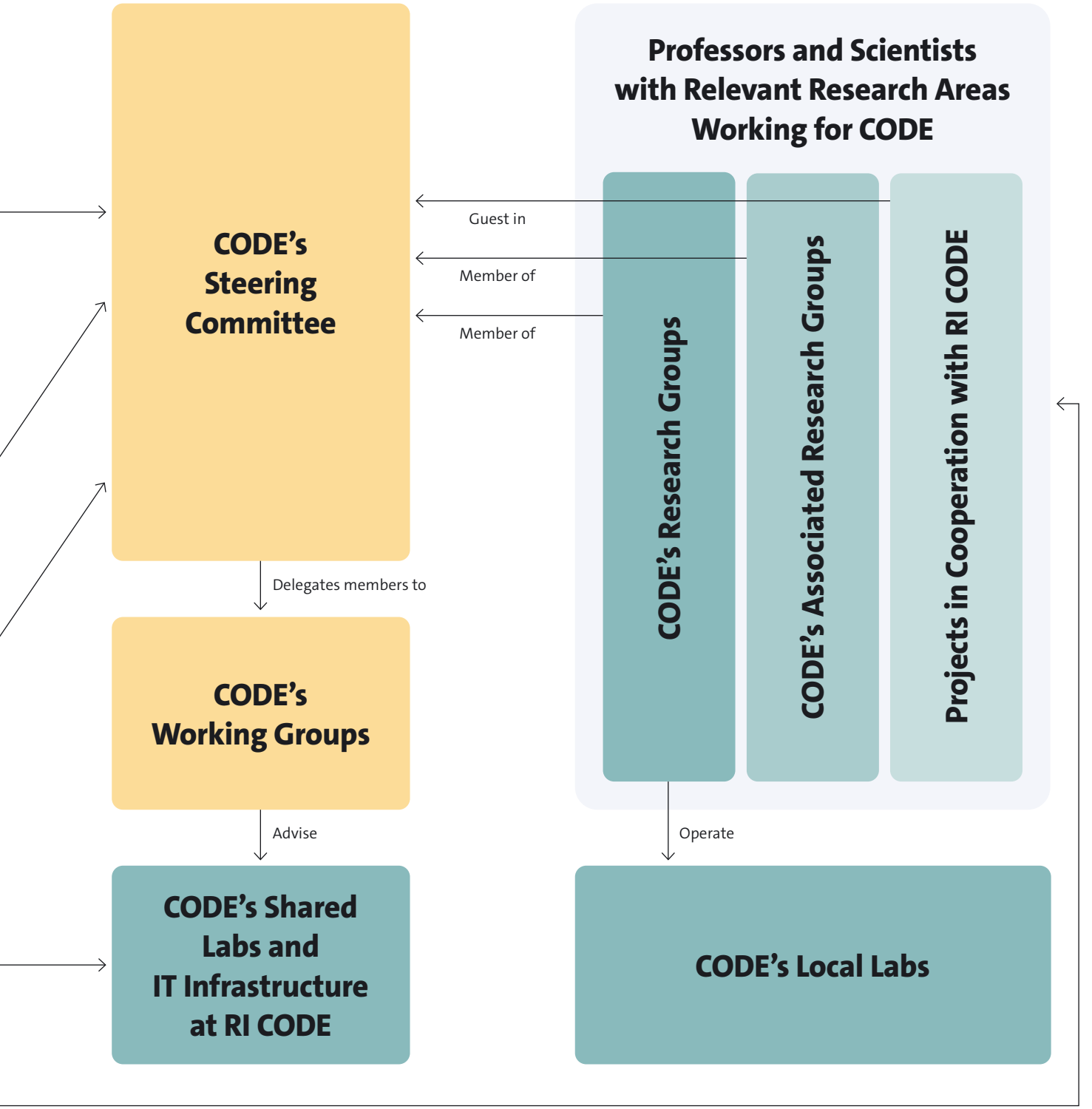
55093 **Penetration Testing Lab**

ADDITIONAL EVENTS

- April 24, 2024, Presentation at the innovation workshop of EAD Energieabrechnungs-Systeme GmbH in Erfurt, Germany
  - Mathias Schlolaut gave an insight into passwords and phishing attacks, supplemented by practical examples.
- October 28, 2024, Conference "Algebraic Number Theory – A workshop for young researchers" at the University of the Bundeswehr Munich
  - Sören Kleine was co-organizer of the event, which gave the mainly young participants the opportunity to present their research to a wider audience.

Organization of RI CODE




CODE's Steering Committee
Professors and Scientists with Relevant Research Areas Working for CODE
Guest in
Member of
Member of
CODE's Research Groups
CODE's Associated Research Groups
Projects in Cooperation with RI CODE
Delegates members to
CODE's Working Groups
Advise
Operate
CODE's Shared Labs and IT Infrastructure at RI CODE
CODE's Local Labs

How to Find Us

Research Institute Cyber Defence and Smart Data (CODE)
University of the Bundeswehr Munich
Carl-Wery-Straße 18
81739 Munich
Germany

code@unibw.de
+49 89 6004 7300
www.unibw.de/code

LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Location Map

Editorial Information

PUBLISHER

Prof. Dr. Wolfgang Hommel,
Prof. Dr. Michaela Geierhos,
Marcus Knüpfer,
Benjamin Bellgrau

Research Institute CODE
University oft he Bundeswehr Munich
Carl-Wery-Str. 18
81739 Munich
Germany

MANAGEMENT OF RI CODE

Prof. Dr. Wolfgang Hommel,
Executive Director

Prof. Dr. Michaela Geierhos,
Technical Director

Marcus Knüpfer, M. Sc.,
Managing Director

PROFESSORS AT RI CODE

Prof. Dr. Florian Alt,
Professor for Usable Security and Privacy (until 10/2024)

Prof. Dr. Harald Baier,
Professor for Digital Forensics

Prof. Dr. Stefan Brunthaler,
Professor for Secure Software Engineering

Prof. Klaus Buchenrieder, PhD,
Professor for Embedded Systems/Computers in Technical Systems

Prof. Dr. Gabi Dreo Rodosek,
Professor for Communication Systems and Network Security

Prof. Dr. Michaela Geierhos,
Professor for Data Science

Prof. Dr. Marta Gomez-Barrero,
Dean of Studies of the Faculty for Computer Science at UniBw M,
Professor for Machine Learning

Prof. Dr. Udo Helmbrecht,
Honorary Professor at RI CODE

Prof. Dr. Wolfgang Hommel,
Dean of the Faculty for Computer Science at UniBw M,
Professor for Software and Data Security

Prof. Dr. Ulrike Lechner,
Professor for Business Informatics

Prof. Dr.-Ing. Mark Manulis,
Vice Dean of the Faculty for Computer Science at UniBw M,
Professor for Privacy

Jun. Prof. Maximilian Moll,
Junior Professor for Operations Research – Prescriptive Analytics

Pro. Dr. Eirini Ntoutsi,
Professor for Open Source Intelligence

Prof. Dr. Stefan Pickl,
Professor for Operations Research

Prof. Dr. Daniel Slamanig,
Professor for Cryptology

Prof. Dr. Gunnar Teege,
Professor for Distributed Systems

Prof. Dr. Arno Wacker,
Professor for Data Privacy and Compliance

MEMBERS OF THE ADVISORY BOARD (IN 2024)

From the Faculty for Computer Science at the University of the Bundeswehr Munich

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

OTHER MEMBERS

Wolfgang Sachs,
Head of Division CIT I.2, Federal Ministry of Defence

Dr. Norbert Gaus,
Executive Vice President of Siemens AG (until 06/2024)

Dr. Ralf Wintergerst,
Chairman of the Management Board of Giesecke + Devrient (until 06/2024)

Dr.-Ing. Christian Keimel,
Airbus Defence and Space (since 07/2024)

Dr. Kai Martius,
Chief Technology Officer, secunet Security Networks AG (since 07/2024)

Prof. Dr. Johann Pongratz,
TU Dortmund

EDITING AND COORDINATION

Benjamin Bellgrau, M. Sc.,
Public Relations Officer

ART DIRECTION

Tausendblauwerk Design Agency
Michael Berwanger

www.tausendblauwerk.de

PROOFREADING

Dr. Michelle Ruth Büscher,
Technical Translator/Editor

PRINTED BY

druckhaus köthen

https://koethen.de

REGULATIONS

Editorial Deadline: March 2025

Title illustration: Adobe Stock / Alexey

ISBN: 978-3-943207-93-4 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-943207-94-1 | ISSN: 2748-9507)
as well as in German
(ISBN: 978-3-943207-91-0 | ISSN: 2748-8780).


der Bundeswehr
Universität München
CODE
RI
Research Institute
Cyber Defence
Universität der Bundeswehr München