Prof. Dr. Christian Zenger

Curriculum Vitae

Summary

- Generated 4.1 Mio. € (total with co-PIs 70.4 Mio. €) funding since 2015
- 2 papers in A+ conferences and journals in 2022
- h-index of 11
- Teaching and continuously improving own lecture since 2016
- +100 Bachelor/Master thesis supervised in the last 10 years
- Co-supervisor of three PhD students since 2018
- +20 collaborations with academic institutes, e.g., Harvard and Princeton
- Founded and bootstrapped an award winning start-up up to 50 people
- Holds 5 patents

Education

01/2013–01/2017 **Dr.-Ing. (summa cum laude) in Physical-Layer Security**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum*, Germany.
- Advisors: Prof. Dr.-Ing. Christof Paar and Prof. Dr. Dr. Holger Boche (TUM)
- Title: *Physical-Layer Security for the Internet of Things*

04/2012–12/2012 **Master's Thesis abroad**, *The Security and Privacy Research (SPQR) Lab, University of Massachusetts*, USA, *Grade: 93%.*
- Advisors: Prof. Christof Paar, Prof. Heiko Knospe and Prof. Wayne Burleson
- Title: *E-cash Schemes on NFC-Smartphones with Applications in Transportation*

09/2010–12/2012 **M.Sc. Electrical Engineering and Computer Science with focus on Communication Systems and Networks (double-degree)**, *TH Cologne and the University of Applied Sciences Bonn-Rhein-Sieg*, Germany, *Grade: 91%.*

04/2010–08/2010 **Bachelor's Thesis**, *Fraunhofer FKIE*, Germany, *Grade: 99%.*
- Advisors: Prof. Dr.-Ing. H. Elders-Boll and Dr.-Ing. M. Adrat
- Title: *An Analytical Comparison of Spectrum Sensing Techniques for Cognitive Radio*

07/2007–08/2010 **B.Sc. Electrical Engineering (with honors, best in class)**, *TH Cologne*, Germany.

09/2005–06/2007 **Abitur**, *Night School AKBK Horrem*, Germany.

09/2002–08/2005 **Completed vocational training as an IT system electronics technician**, *RWE Power AG and AKBK Horrem*, Germany.

Academic positions

04/2016–04/2023 **Junior Professor**, *Secure Mobile Networking*, Ruhr University Bochum, Germany.
- I am employed as a Junior Professor at the Ruhr University Bochum. I work at the Division of Digital Communication Systems of the Department of Electrical Engineering & Information Technology (ETIT) and I am based at campus in Bochum, Germany.

02/2023–Present **Lecturer**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum.*

- Wireless Physical-Layer Security (bachelor and master lecture). In this course students are introduced to fundamental concepts and applied aspects of wireless physical-layer security. In this course, two topics are developed. First, the participants of the internship learn the basics about Software Defined Radios (SDRs). Already after the first lecture the students are able to develop passive eavesdropping with GNU Radio for the RTL-SDR architecture. During the following dates, knowledge of the SDR architecture and radio standards will be deepened. In addition, the students have to write more and more complex programs as homework. In the second part of the course, the students learn how to use radio channel-based security architectures like channel-based key generation and channel-based fingerprinting. The students are then divided into groups of three people. Each group receives a measurement setup based on three Raspberry Pis, wireless modules and measurement software, as well as a virtual machine with a preconfigured evaluation framework. Each group implements a given channel-based security architecture (a different one every year) in Python, and has to get it running in the evaluation framework under realistic conditions.

02/2013–Present **Thesis Supervisor**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum.*

- Supervision of students during seminars, Bachelor and Master theses.
- Since 2018, supervision of two PhD students, together with Prof. Paar.

02/2013–10/2015 **Teaching Assistant**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum.*

- Lecturer of the course *Introduction in Cryptography I&II* (bachelor lecture). In this course students are introduced to fundamental concepts of cryptography and data security. The first part of the lecture deals with historical-, stream-, and, block ciphers. The main part of the lecture is dedicated to the symmetric ciphers DES and AES. At the end of the course the asymmetric scheme RSA is discussed. In addition to the cryptographic algorithm we introduce the necessary mathematical fundamentals (rings of integers, extended euclidean algorithm, finite field). The second part enfolds asymmetrical schemes based on the discrete-logarithm problem (Diffie-Hellman key exchange, ElGamal encryption, elliptic curve cryptography) as well as digital signatures, message authentication codes, hash function (SHA-3), certificates, key exchange protocols, and security services.
- Supported lectures with exercises in cryptography and software/hardware implementations.

09/2010–04/2012 **Adjunct Lecturer**, *Institute of Communications Engineering, Cologne University of Applied Science.*

- Lecturer of the course *Signals and Systems Theory I & II* (bachelor class)

Work Experience

04/2016–Present **Co-Founder & CEO**, *PHYSEC GmbH*, Germany.
I co-founded PHYSEC based on the work from my PhD. PHYSEC is a Bochum based, leading deep-tech company in physical-layer security to secure the Internet of Things.

01/2021–Present **Board Member**, *Kompetenzzentrum Digitale Wasserwirtschaft*, Germany.
The vision of the KDW is an agile water management system that uses digitization to master current and future challenges such as climate change, economic and social changes and, last but not least, the shortage of skilled workers.

09/2019–Present **Member of Scientific and Technical Advisory Board**, *Cube5*, Germany.
The incubator Cube 5 supports students and start-ups in the field of IT security from the development of ideas through technology development to the later establishment of a company.

02/2016–Present **Lecturer**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum*, Germany.
Teaching on academic level. Giving lectures in Wireless Physical-Layer Security (bachelor and Master).

02/2017–06/2021 **Post-Doc, Team Lead**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum*, Germany.
Leading an international research project on Radio-Wave based Virtual Proof of Reality for Nuclear Warhead Disarmament and Inspection Scenarios. The project is a joint project with Harvard University, Princeton University, and PHYSEC GmbH.

10/2015–12/2019 **Board Member**, *Horst Görtz Institute for IT Security*, Germany.
The Horst Görtz Institute for IT Security (HGI), Research Department of the Ruhr University Bochum, was founded in 2002 to address shortcomings in IT security research in Europe as a whole. The HGI currently hosts 26 professors and their teams.

01/2013–01/2017 **Research Assistant/PhD Student**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum*, Germany.
Worked on the 'Providing Physical Layer Security for the Internet of Things (PROPHYLAXE)' project (supported in part by the German Federal Ministry for Education and Research) and follow-up research. Supervised student trainees and several final theses. Supported lectures with exercises in cryptography and software/hardware implementations.
- Research Area: Physical layer security, hardware security, embedded security, communications engineering, system design
- Advisors: Prof. Dr.-Ing. Christof Paar & Prof. Dr.-Ing. Tim Güneysu
- Core Area: Prototyping efficient security systems based on physical layer security, focus on side-channel resistance and performance

04/2012–12/2012 **Master's Thesis**, *The Security and Privacy Research (SPQR) Lab, University of Massachusetts, Amherst*, USA, *Grade: 93%.*
- Advisors: Prof. Dr.-Ing. Christof Paar, Prof. Dr. rer. nat. Heiko Knospe, and Prof. Dr. Wayne P. Burleson
- Title: *Evaluation of E-cash Schemes on NFC-Smartphones with Applications in Public Transportation*
- Description: Efficient implementation of Brands and ACL e-cash schemes with attributes on an NFC smartphone. Development of a subtle technique to make use of the ECDHKeyAgreement class that is available in the BlackBerry API (and in the API of other systems) and show how the schemes can be implemented efficiently to satisfy the tight timing imposed by the transportation setting.

05/2011–04/2012 **Intern**, *Chair for Embedded Security, Horst Görtz Institute for IT Security, Ruhr University Bochum*, Germany.
Electromagnetic Side-Channel Attacks on RSA Implementations of Smartphone Processors. Developing a new tool for finding side-channels: 2^{nd} order cyclostationary feature detection algorithm.

09/2010–04/2012 **Embedded System Development Engineer**, *Department of Digital Signal Processing and Motion Control, TH Cologne*, Germany.
Electric power interface for agricultural tractors and implements: Developing a decentralized industrial servo drive system with minimized cables and connectors. Implementation of FPGA-based EtherCAT-Slave-Systems combined with a Powerline Communication System. TCP/IP-stack implementation on a softcore processor (Altera Cyclone III). The project was in cooperation with the industrial companies: Altera Deutschland, EBV Elektronik GmbH & Co., John Deere GmbH & Co KG, and Beckhoff Automation GmbH.

04/2010–09/2010 **Student Assistant**, *Fraunhofer Institute for Communication, Information Processing and Ergonomics*, Wachtberg, Germany.
Department of Communication Systems, Area Software Defined Radio (on behalf of the NATO and the EDA).

09/2009–09/2010 **Student Assistant**, *Department of Information, Media and Electrical Technology of Cologne University of Applied Science*, Cologne, Germany.
Technical assistance to the dean of the department.

02/2009–12/2009 **Intern**, *DataCollect GmbH*, Kerpen, Germany.
Error analysis of a mobile radar system in a cold chamber measurement setup.

04/2010–09/2010 **Bachelor's Thesis**, *Fraunhofer Institute for Communication, Information Processing and Ergonomics*, Germany, *Grade: 99%*.
- Advisors: Prof. Dr.-Ing. H. Elders-Boll & Dr.-Ing. M. Adrat
- Title: *An Analytical Comparison and Evaluation of Existing Spectrum Sensing Techniques for Cognitive Radio*
- Description: Implementation of spectrum sensing techniques. We developed an algorithm to find adaptively the optimal parameter for the uncertainty principle of the sliding DFT as well as an 2^{nd} order cyclostationary feature detection algorithm.

08/2007–08/2009 **Student assistant**, *Solutions for Media GmbH*, Cologne, Germany.
Main tasks:
- System setup during international fairs and events
- Server and laboratory administration
- Software developer of smaller tasks (Java, C#)

04/2007–08/2007 **IT consultant**, *RTL Television*, Cologne, Germany.
Problem management and 2nd Level technical support of broadcast specific software and hardware.

11/2005–04/2007 **IT consultant**, *West German Broadcasting*, Cologne, Germany.
2nd Level technical support of broadcast specific software and hardware. Problem management based on ITIL v2.

09/2002–08/2005 **Apprenticeship as IT system technician**, *RWE Power AG*, Germany.

Honors & Awards

12/2022 **European Innovation Council — Seal of Excellence**.
06/2022 TeleTrust Innovation Award 2022
12/2021 European Innovation Council — Seal of Excellence.
02/2021 Winner of ESCO's European Cybersecurity STARtup Award 2021.
11/2020 Innovation and growth award by city of Bochum.
09/2020 The Most Admired Company of the Year 2020 Award.
04/2020 RED HERRING Award, Europe 2020.
06/2019 1^{st} place "NRW Gründerpreis" by MWIDE (30,000 €).
12/2018 **MIT Technology Review 2018: Innovator under 35**.
10/2018 1^{st} place in **German IT-Security Award 2018** (100,000 €).
06/2018 MIT Technology Review 2018: Innovator under 35 - Germany.
06/2018 1^{st} place "Digital Start-up of the year 2018" by BMWi (50,000 €)
03/2017 Winner of the 1^{st} place of BMWi Digitale Innovation (32,000 €).
02/2017 Received EXIST Forschungstransfer II grand (180,000 €).
01/2017 PhD with honors (summa cum laude).
06/2016 Winner of eco Internt Security Award — Category: Next Generation Security.
04/2016 1^{st} place of Senkrechtstarter (15,000 €).
04/2016 Winner of innovation award 2016 by Ruhr University Bochum.
10/2015 Received EXIST Forschungstransfer I grand (650,000 €).
09/2014 1^{st} place of the innovation competition Gründercampus Ruhr 2014
04/2012 Received a scholarship from the German Academic Exchange Service.
08/2010 Earned an award for the best Bachelor's graduation of the class 2010.

Inventions

[P5] **Zenger, C.** and Jansen, K., 2022. Verfahren zur automatischen Durchführung von physischen Kontrollen von elektronischen Geräten unter Berücksichtigung von latent unsicheren Lieferketten und Betriebsumgebungen. DPMA: DE102022102911.

[P4] **Zenger, C.**, Jansen, K. and Zimmer, J., 2020. Verfahren zur Etablierung einer Relay Station Attack geschützten Funkverbindung. DPMA: DE102020104918.

[P3] **Zenger, C.**, Wans, S. and Paar, C., 2017. Verfahren zur Etablierung einer sicherern Ende-zu-Ende Verbindung über LoRa(WAN). DPMA: DE102017117170.

[P2a,P2b,P2c,P2d] **Zenger, C.**, 2017. Verfahren zur Prüfung der Integrität einer dedizierten physikalischen Umgebung zum Schutz von Daten. DPMA: DE102017114010 , PCT2018/066605, EP18740516.2-1218, US16/626,313.

[P1] **Zenger, C.**, 2016. Verfahren für den Betrieb eines cyber-physischen Informationsübermittlungsystems. DPMA: DE102016109721.

Peer-Reviewed Journal Papers

[J3] Li, G., Hu, L., Staat, P., Elders-Boll, H., **Zenger, C.**, Paar, C. and Hu, A., to appear in 2022, Reconfigurable Intelligent Surface for Physical Layer Key Generation: Constructive or Destructive? In IEEE Wireless Communications Magazine.

[J2] **Zenger, C.**, Pietersz, M., Zimmer, J., Posielek, J.F., Lenze, T. and Paar, C., 2016, Authenticated key establishment for low-resource devices exploiting correlated random channels. In Computer Networks, 109, pp.105-123.

[J1] **Zenger, C.**, Zimmer, J. and Paar, C., 2015. Security analysis of quantization schemes for channel-based key extraction. In EAI Endorsed Transactions on Security and Safety.

Peer-Reviewed Conference Papers

[C21] Staat, P., Heinrichs, M., Elders-Boll, H., **Zenger, C.** and Paar, C., 2022. Mirror Mirror on the Wall: Wireless Environment Reconfiguration Attacks Based on Fast Software-Controlled Surfaces ASIA CCS '22: ACM Asia Conference on Computer and Communications Security.

[C20] Staat, P., Jansen, K., Elders-Boll, H., **Zenger, C.** and Paar C., 2022. Analog Physical-Layer Relay Attacks with Application to Bluetooth and Phase-Based Ranging, WiSec '22: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks.

[C19] Staat, P., Tobisch, J., **Zenger, C.** and Paar, C., 2022. Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems. In IEEE Symposium on Security and Privacy.

[C18] Staat, P., Elders-Boll, H., Heinrichs, M., Kronberger, R., **Zenger, C.** and Paar, C., 2021. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (pp. 745-751).

[C17] Li, C., Brauer, J., Sezgin, A. and **Zenger, C.**, 2021. Kalman filter based MIMO CSI phase recovery for COTS WiFi devices. In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (pp. 4820-4824).

[C16] Zimmer, P., Weinreich, R., **Zenger, C.**, Sezgin, A. and Paar, C., 2021. Keys from the Sky: A First Exploration of Physical-Layer Security Using Satellite Links. In ICC IEEE International Conference on Communications (pp. 1-7).

[C15] Tobisch, J., **Zenger, C.** and Paar, C., 2020. Electromagnetic enclosure PUF for tamper proofing commodity hardware and other applications. In Design, Automation and Test in Europe Conference (DATE) — Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE).

[C14] Vogt, H., Li, C., Sezgin, A. and **Zenger, C.**, 2019. On the precise phase recovery for physical-layer authentication in dynamic channels. In IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6).

[C13] **Zenger, C.**, Pietersz, M., 2018. IoT-Security and Product Piracy: Smart Key Management versus Secure Hardware. In Embedded World Conference.

[C12] **Zenger, C.**, Pietersz, M., Rex, A., Brauer, J., Dressler, F.P., Baiker, C., Theis, D. and Paar, C., 2017. Implementing a real-time capable WPLS testbed for independent performance and security analyses. In 51st Asilomar Conference on Signals, Systems, and Computers (pp. 9-13).

[C11] **Zenger, C.**, Vogt, H., Zimmer, J., Sezgin, A. and Paar, C., 2016. The passive eavesdropper affects my channel: Secret-key rates under real-world conditions. In IEEE Globecom Workshops (GC Wkshps) (pp. 1-6).

[C10] **Zenger, C.**, Zimmer, J., Pietersz, M., Driessen, B. and Paar, C., 2016. Constructive and destructive aspects of adaptive wormholes for the 5g tactile internet. In Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 109-120).

[C9] **Zenger, C.**, Pietersz, M. and Paar, C., 2016. Preventing relay attacks and providing perfect forward secrecy using physec on 8-bit µc. In 2016 IEEE International Conference on Communications Workshops (ICC) (pp. 110-115).

[C8] **Zenger, C.**, Zimmer, J., Pietersz, M., Posielek, J.F. and Paar, C., 2015. Exploiting the physical environment for securing the internet of things. In Proceedings of the 2015 New Security Paradigms Workshop (pp. 44-58).

[C7] Guillaume, R., Winzer, F., Czylwik, A., **Zenger, C.** and Paar, C., 2015. Bringing PHY-based key generation into the field: An evaluation for practical scenarios. In IEEE 82nd Vehicular Technology Conference (VTC2015-Fall) (pp. 1-5).

[C6] **Zenger, C.**, Zimmer, J., Posielek, J.F. and Paar, C., 2015. On-line entropy estimation for secure information reconciliation. In proceedings of the 12th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services on 12th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 254-259).

[C5] **Zenger, C.**, Ambekar, A., Winzer, F., Pöppelmann, T., Schotten, H.D. and Paar, C., 2014. Preventing scaling of successful attacks: A cross-layer security architecture for resource-constrained platforms. In International Conference on Cryptography and Information Security in the Balkans (pp. 103-120).

[C4] **Zenger, C.**, Chur, M.J., Posielek, J.F., Paar, C. and Wunder, G., 2014. A novel key generating architecture for wireless low-resource devices. In IEEE International Workshop on Secure Internet of Things (pp. 26-34).

[C3] Guillaume, R., Mueller, A., **Zenger, C.**, Paar, C. and Czylwik, A., 2014. Fair comparison and evaluation of quantization schemes for phy-based key generation. In 18th International OFDM Workshop (InOWo'14) (pp. 1-5).

[C2] Kasper, T., Kühn, A., Oswald, D., **Zenger, C.** and Paar, C., 2013. Rights management with NFC smartphones and electronic ID cards: A proof of concept for modern car sharing. In International Workshop on Radio Frequency Identification: Security and Privacy Issues (pp. 34-53).

[C1] Hinterwälder, G., **Zenger, C.**, Baldimtsi, F., Lysyanskaya, A., Paar, C. and Burleson, W.P., 2013. Efficient e-cash in practice: NFC-based payments for public transportation systems. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 40-59).

Books and Book Chapters

[B2] Börner, M., Koepke, H. and **Zenger, C.**, 2022. Sichere Bits und Atome: IoT im Spannungsfeld zwischen Cyber- und Physischer-Sicherheit. In: Christian Vogt, Patrick Hennies, Christian Endreß, Patrick Peters (Hrsg.), Wirtschaftsschutz in der Praxis. Herausforderungen an die Sicherheit im Zeitalter von Digitalisierung und Krise (S. 245-262). Springer.

[B1] **Zenger, C.**, 2017. Physical Layer Security for the Internet of Things, Dissertation, Ruhr University Bochum.

Research Grants

[G17] BMBF **6G-ANNA: 6G-Industrieprojekte zur Erforschung von ganzheitlichen Systemen und Teiltechnologien für den Mobilfunk der 6. Generation**, 2022-2025, co-PI, with Dr. Marco Hoffmann (Nokia), Rainer Woytaszek (AIN), Stephanie Strassner (Airbus), Daniel Günzel (Blackned), Dr. Andreas Müller (Bosch), Andreas Dotzler (Cadami), Dr. Michael Meyer (Ericsson), Prof. Norman Franchi (Friedrich-Alexander-Universität Erlangen-Nürnberg), Prof. Slawomir Stanczak (HHI), Niels König (FhG-IPT), Christian Banse (FhG-AISEC), Prof. Martina Zitterbart (KIT), Sreekrishna Pandi (Meshmerize), Ievgenii Tsokalo (Mimetik), Prof. Sanaz Mostaghim (Otto-von-Guericke-Universität Magdeburg), Andreas Roessler (Rohde & Schwarz), Prof. Aydin Sezgin (RUB), Prof. Haris Gačanin (RWTH), Prof. Anke Schmeink (RWTH), Dr. Arne Broering (Siemens), Dr. Claus Keuker (Smart Mobile Labs), Prof. Admela Jukan (Technische Universität Braunschweig), Prof. Christian Wietfeld (Technische Universität Dortmund), Prof. Frank H.P. Fitzek (Technische Universität Dresden), Prof. Gerhard Fettweis (Technische Universität Dresden), Prof. Gerhard Bauch (Technische Universität Hamburg), Prof. Hans D. Schotten (Technische Universität Kaiserslautern), Prof. Wolfgang Kellerer (Technische Universität München), Prof. Eckehard Steinbach (Technische Universität München), Prof. Georg Carle (Technische Universität München), Prof. Armin Dekorsy (Universität Bremen), Dr. Ralf Irmer (Vodafone), Christian Piechnick (Wandelbots).

[G16] BMBF **UltraSec: Sicherheitsarchitektur für eine UWB-basierte Anwendungsplattform**, 2022-2025, co-PI, with Prof. Dr. Slawomir Stanczak (Fraunhofer HHI), Prof. Dr.-Ing. Gerhard Wunder (FU Berlin), Prof. Dr. Marian Margraf (FU Berlin), Dr. Olaf Dressel (Bundesdruckerei), Dr. Ralf Dietl (NC Systems), Dr. Eric Wichterich (Katholisches Klinikum Bochum).

[G15] BMBF **C-ray4edge: Cyber-physikalische Sicherheit mittels Radiometrie für den Edge**, 2022-2025, co-PI, with Prof. Dr.-Ing. Matthias Waehlisch (FU Berlin), Prof. Dr. Thomas Schmidt (HAW Hamburg), Prof. Dr. Gunnar Schomaker (WestfalenWIND IT).

[G14] BMBF **ProPair: Kontext-basierte Vertrauensinitialisierung telemedizinischer Kleinstgeräte**, 2021-2024, co-PI, with Prof. Dr.-Ing. Amir Moradi (Uni Köln), Dr. Eimo Martens (TUM), Dr.-Ing. Johannes Kreuzer (Cosinuss).

[G13] BMBF **Smart Green City**, 2022-2025, co-PI, with Prof. Dr.-Ing. André Niemann (Uni-Dui), Dr. Benjamin Mewes (Okeanos).

[G12] BMBF **5G-Furios: Resiliente und taktile 5G-Ende-zu-Ende Infrastruktur für Privacy- und Safety-proofed Remote Assistance und Worker Safety**, 2022-2025, co-PI, with Prof. Dr.-Ing. Aydin Sezgin (RUB), Dr. Eike Permin (SMS Digital), Dr. Markus Große Böckmann (oculavis), TMR - Telekommunikation Mittleres Ruhrgebiet GmbH (TMR).

[G11] BMBF **5Guarantee: Agiles System für Ende-zu-Ende-Leistungsgarantien in lokalen 5G Netzen ganzheitlich eingebettet in die Industrie-4.0-Prozesslandschaft** , 2019-2022, co-PI, with Prof. Dr.-Ing. Christian Wietfeld (TU Dortmund), Prof. Dr.-Ing. Bernd Kuhlenkötter (RUB), Dr.-Ing. Patrick-Benjamin Bök (Weidmüller), Dr. Arnt Vienenkötter (Miele), Dr. Andreas Lewandowski(Comnovo), Dr. Cara Schwarz-Schilling (WIK-Consult).

[G10] BMBF **PHY2APP: Erweiterung von Physical Layer Security für Ende-zu-Ende Absicherung des IoT**, 2021-2023, co-PI, with Prof. Dr.-Ing. Gerhard Wunder (FU Berlin), Axel Schüßler (IoT Connect).

[G9] BMBF **TinyPART: Tiny, private, proved and isolated**, 2021-2024, co-PI, with Prof. Dr.-Ing. Gerhard Wunder (FU Berlin), Prof. Dr. Emmanuel Baccelli (INRIA), Prof. Dr. Gilles Grimaud (Univerisity of Lille), Chrystel Gaber (Orange).

[G8] BMWi **GUARD: Erkennen von Angriffen durch Nutzung radiometrischer Geräteprofilen und maschinellem Lernen auf ressourcenbeschränkten IoT-Mikrocontrollern**, 2020-2022, co-PI, with Prof. Dr. Asja Fischer (RUB).

[G7] BMBF **MetaSEC: Physical-Layer Security für IoT-Kleinstgeräte unter Nutzung rekonfigurierbarer Metaoberflächen**, 2020-2023, co-PI, with Prof. Dr.-Ing. Aydin Sezgin (RUB), Prof. Dr.-Ing. Rainer Kronberger (TH Köln).

[G6] BMBF **mINDFUL: Intrusion Detection Architektur durch Fusion mit physikalischen Sensordaten mittels künstlicher Intelligenz und datenschutzkonforme Aggregation für IT-Sicherheit in der Industrie 4.0**, 2020-2023, co-PI, with Prof. Dr. Asja Fischer (RUB), Prof. Dr.-Ing. Aydin Sezgin (RUB), Prof. Dr.-Ing. Amir Moradi (Uni Köln), Dr.-Ing. Sebastian Ruthe (logarithmo).

[G5] BMWi **5Gain: 5G Infrastrukturen für Zellulare Energiesysteme unter Nutzung künstlicher Intelligenz**, 2019-2022, co-PI, with Prof. Dr.-Ing. Christian Wietfeld (TU Dortmund), Prof. Dr. Christian Rehtanz (TU Dortmund), Prof. Christa Reicher (RWTH), Dr. Andreas Wirsen (Fraunhofer ITWM), Dr. Jan Rettberg (Stadt Dortmund), Paul Dittrich (urban Energy), Sven Baumgarte (DEW21), Dr. Angela Carell (adesso AG).

[G4] BMBF **ReMiX: Resilienz in Mixed-Criticality Systemen des Industriellen Internet der Dinge**, 2019-2021, co-PI, with Prof. Dr.-Ing. Aydin Sezgin (RUB), Prof. Dr. Sebastian Steinhorst (TUM), Prof. Dr. Naim Bajcinca (TU Kaiserslautern), Dr.-Ing. Dirk Kuschnerus (Krohne Innovation GmbH).

[G3] BMBF **SecuFog: Sichere Fog-Verbindungschicht für IoT Anwendungen**, 2017-2020, co-PI, with Prof. Dr.-Ing. Adam Wolisz (TU Berlin), Prof. Dr. Marian Margarf (FU-Berlin), Dirk Sommerfeld (azeti Networks AG).

[G2] BMWI **EXIST Forschungstransfer: PHYSEC (Phase 2)**, 2015-2017

[G1] BMWI **EXIST Forschungstransfer: PHYSEC (Phase 1)**, 2015-2017

Bochum, 01.02.2023.