

6G-PHYSEC TRAINING SCHOOL PROGRAM OUTLINE



May 19 & 20, 2026 @ Johannes Kepler University, Austria



Presenter: Bernhard Etzlinger

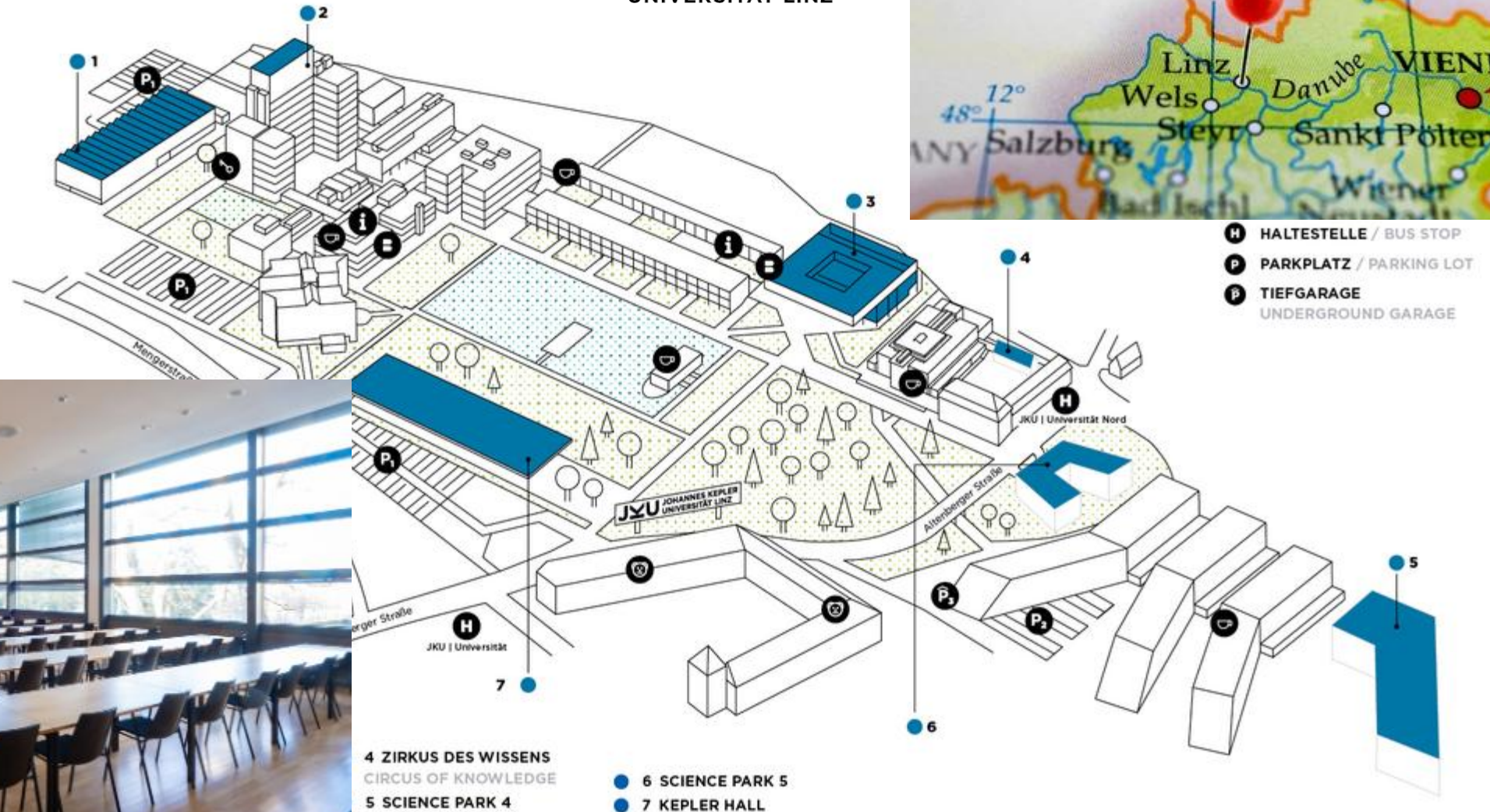
Date: 15.04.2026



TS at JKU Linz

JKU
JOHANNES KEPLER
UNIVERSITÄT LINZ

- May 19&20
- 57 participants
- 5 trainers



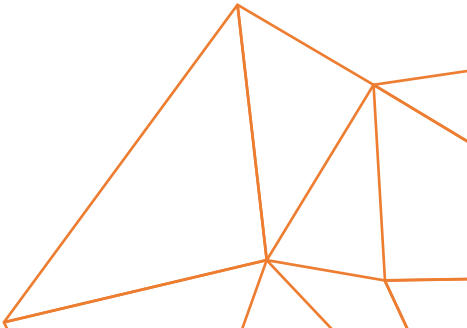
4 ZIRKUS DES WISSENS
CIRCUS OF KNOWLEDGE
5 SCIENCE PARK 4

6 SCIENCE PARK 5
7 KEPLER HALL



Tuesday, 19.5.2026	
08:00	Registration
08:30	Welcome and Overview of Training School in the context to Trustworthy 6G Bernhard Etzlinger (JKU)
09:00	6G Security Research and the Role of Security in Era of AI-RAN Pawani Porambage (VTT)
11:00	Coffee Break
11:30	Resilient 6G communications, part 1 Akshay Jain (ConfidentialMind Oy)
12:30	Lunch Break
14:00	Resilient 6G communications, part 2 Akshay Jain (ConfidentialMind Oy)
15:00	Coffee Break
15:30	Device Authentication for Internet of Things Junqing Zhang (Univ. of Liverpool)
17:30	End of Day 1
19:00	Dinner in City Center (optional)

Wednesday, 20.5.2026	
08:30	Registration
09:00	TRICK: Time and Range Integrity Checks, part 1 Mridula Singh (CISPA)
10:30	Coffee Break
11:00	TRICK: Time and Range Integrity Checks, part 2 Mridula Singh (CISPA)
12:30	Lunch Break & University Tour
14:30	Hardware Security, part 1 Thomas Korak (Infineon)
16:00	Coffee Break
16:30	Hardware Security, part 2 Thomas Korak (Infineon)
18:00	End-of-School / Get Together (optional)





Pawani Porambage

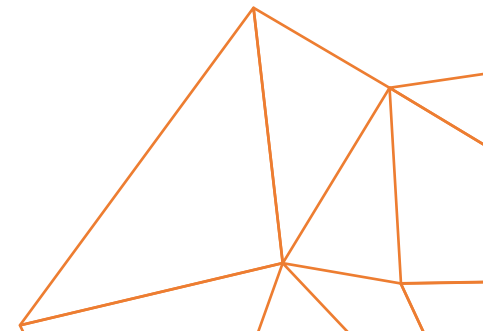


She is a Senior Scientist at VTT Technical Research Centre of Finland and an Adjunct Professor at University of Oulu. She received the Doctoral degree in wireless sensor network security from the University of Oulu, Finland, in 2018. Her research interests fall under mobile network security topics that entail 5G/6G, Open RAN, and AI-RAN.

Topic: 6G Security Research and the Role of Security in Era of AI-RAN

Sustainability and trustworthiness are heavily considered in the pathway towards 6G. The first half of the talk will provide an overview on 6G security research and future directions at both European and Global levels. The evolution of threat landscape in the mobile networks and the associated technologies will be presented as an overview. The second half will focus on the role of security research with the wide adaptation of AI in the Radio Access Networks. This segment will share insights on new research directions and introduce challenges as the attack surface evolves due to the architectural and functional changes envisioned with AI-RAN.

Talk duration: 2h





Akshay Jain



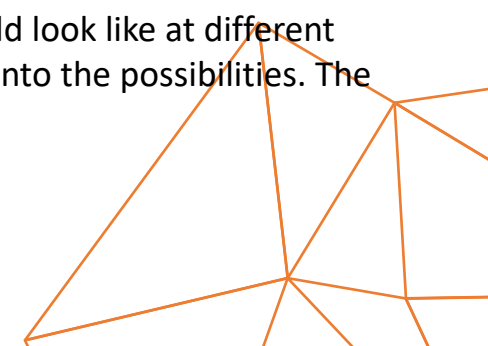
He is a Senior AI Research Engineer at ConfidentialMind Oy where he specializes on Trustworthy, Explainable and Sovereign AI deployment and orchestration for mission-critical scenarios and enterprises. Before joining ConfidentialMind Oy he was also a Senior Research Scientist at Nokia Bell Labs, where he pioneered solutions in defense communications, artificial intelligence, and sustainability for wireless networks. He holds a PhD in Wireless Communication as a Marie Skłodowska-Curie Fellow from Universitat Politècnica de Catalunya in Spain. His research focuses on Trustworthy, Sovereign and Explainable AI, AI/ML methods with next-generation wireless systems, resiliency mechanisms across 5G/6G RAN, Core and management and orchestration plane, and sustainable 6G system design methodologies.

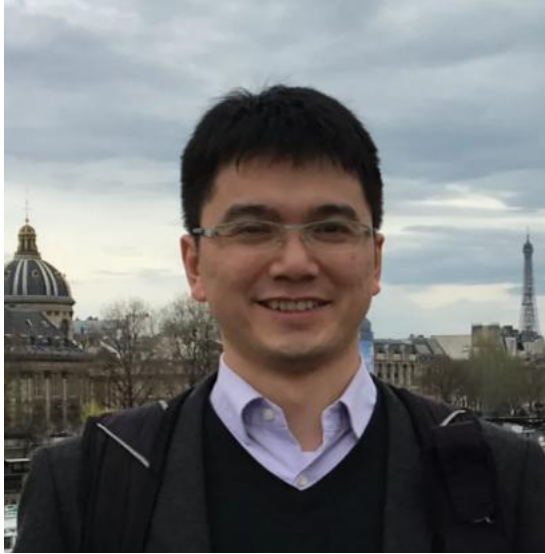
Topic: Resilient 6G communications

pre-lunch session: Discussion on the evolution of 6G, and how resilience will be an important functional component of 6G, which will in turn help in making our societies resilient to the known-unknowns and the unknown-unknowns. In this session, we will delve into what the 6G will look like, what are the specific areas in resilience that 6G standardization is focusing on and what are the opportunities for researchers to create an impact on, i.e., open areas.

post-lunch session: Continuing from the high level discussion, in this session we will delve into the specifics of what resilience could look like at different layers and blocks of a 6G system. This will still be a slightly higher level view with some specific results, but it will provide insights into the possibilities. The session aims to create an engaging atmosphere on what are the potential areas for Resilient 6G research.

Talk duration: 2h





Junqing Zhang



UNIVERSITY OF
LIVERPOOL



Junqing Zhang is Senior Lecturer at University of Liverpool

His work focuses on developing innovative and practical physical layer security solutions for next-generation wireless systems, aiming for ultra-low energy consumption alongside strong security guarantees. He also explores novel wireless sensing applications using Wi-Fi and mmWave radars. His research leverages a wide range of Internet of Things technologies, including IEEE 802.11a/g/n/ac/ax, LoRa/LoRaWAN, Bluetooth, and IEEE 802.15.4/ZigBee, with particular emphasis on the physical and MAC layers.

Topic: Device Authentication for Internet of Things: A Deep Learning-Based Radio Frequency Fingerprint Identification Approach

Internet of Things (IoT) is a disruptive technology that has been fundamentally transforming our everyday life, including many exciting applications such as smart cities, smart homes, connected healthcare, etc. The transformative revolution is enabled by massive low cost and connected devices. Device authentication is vital to grant network access to legitimate devices and reject malicious attackers. Conventional authentication schemes rely on complex cryptographic solutions which may not be suitable for lightweight IoT devices. There is an emerging technique, namely radio frequency fingerprint identification (RFFI), which exploits unique and stable hardware impairments of wireless transceivers as device identifiers. This tutorial will start with the challenges of wireless security and the limitations of existing solutions when applied to IoT. It will then cover different aspects of RFFI, including hardware impairments modelling, deep learning-based RFFI design, and construction of RFFI systems. The tutorial will conclude with existing challenges and visions.

Talk duration: 2h





Mridula Singh



CISPA
HELMHOLTZ-ZENTRUM FÜR
INFORMATIONSSICHERHEIT



Mridula Singh is a tenure-track faculty member at the CISPA Helmholtz Center for Information Security in Saarbrücken, Germany. Her primary research focus is systems security and wireless security, with emphasis on practical attacks and deployable defenses. Her work on physical-layer Message Time-of-Arrival Codes has been used for securing passive keyless entry and start systems in commercial vehicles.

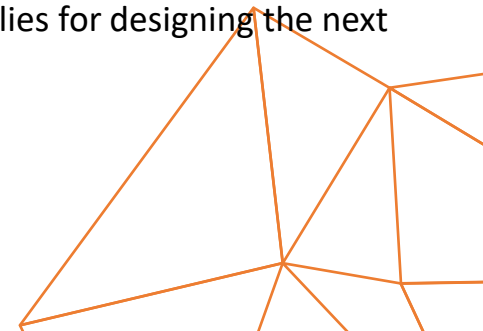
She is currently working on securing sensing modalities for autonomous vehicles and designing scalable positioning systems.

Topic: TRICK: Time and Range Integrity Checks

Wide-area positioning is foundational to applications ranging from aviation and maritime operations to drones and connected vehicles, yet the signals we rely on, especially GNSS, remain susceptible to spoofing attacks.

In this lecture, we will build **intuition for what “secure positioning” means** and **why it is harder than simply adding cryptography to existing systems**. We will then look at **verifiable multilateration (VM) as a representative secure positioning technique**: VM forms a constrained geometric region using multiple two-way ranging (TWR) interactions, but its reliance on uplink receptions makes it difficult to deploy at a wide-area scale. We then **introduce TRICK**, a technique that **bridges this gap by allowing authenticated broadcast signals to contribute in secure region formation**, while requiring only a minimal number of TWR measurements. We close by discussing what TRICK changes for practical secure coverage at scale, and what it implies for designing the next generation of secure wide-area positioning systems.

Talk duration: 3h





Thomas Korak



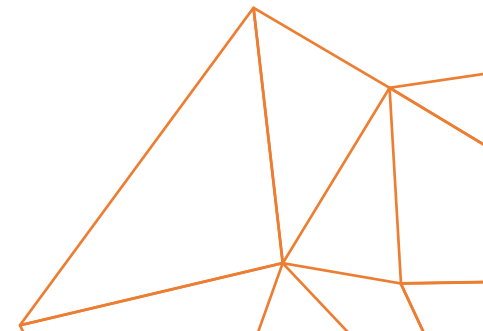
Thomas Korak is a Senior Staff Engineer for Security Evaluation at Infineon Technologies AG.

He is a member of the Product Security (PS) group within the Connected Secure Systems (CSS) division, located in Munich, Germany. His tasks include evaluating the security of products for connected systems and identifying critical issues during the development process. In the evaluation phase, his focus is on physical attacks (e.g. fault injection or side-channel analysis). He is also involved in the development of countermeasures against this type of threat and supports certification processes to meet regional cybersecurity and regulatory requirements.

Topic: Hardware Security: Attacks and Countermeasures

- Types of physical attacks and why they matter
 - Examples of real-world exploits
 - Hardware attack surface / Prerequisites / Threat model /
- Side-Channel Analysis (SCA)
 - Fundamentals (What is side-channel leakage?; Timing, Power, EM, Photon Emission)
 - Equipment and Lab Setup
- Fault Injection (FI)
- Fundamentals (Fault Models; Voltage/Clock Glitching, EM Fault Injection, Laser Fault Injection)
 - Equipment and Lab Setup
- Countermeasures
 - Software vs. Hardware
 - Integrity vs. Confidentiality

Talk duration: 3h



See you in Linz!

