Lukas Struppek

German Research Center for Artificial Intelligence
Technical University of Darmstadt
Darmstadt, Germany

🌐 lukasstruppek.github.io
lukas-struppek
LukasStruppek

Education

- **Technical University of Darmstadt** *2021–Today*
  Ph.D. in Artificial Intelligence and Machine Learning Expected: Early 2025
- **Karlsruhe Institute of Technology (KIT)** *2018–2020*
  M.Sc. in Industrial Engineering and Management Grade: 1.1 (GPA: 3.9), with distinction
- **Karlsruhe Institute of Technology (KIT)** *2015–2018*
  B.Sc. in Industrial Engineering and Management Grade: 1.1 (GPA: 3.9), with distinction

Relevant Experience

- **German Research Center for Artificial Intelligence (DFKI)** *2024–Today*
  Research Scientist for Foundations of Trustworthy AI Systems Darmstadt
- **Karlsruhe Institute of Technology (KIT)** *2018–2020*
  Research Assistant in the Applied Technical-Cognitive Systems Group Karlsruhe
- **Baden-Wuerttemberg Cooperative State University (DHBW)** *2019–2021*
  Lecturer in Software Engineering for Students of Information Systems Karlsruhe

Selected Publications

[1] Hintersdorf, D., **Struppek, L.**, Kersting, K., Dziedzic, A., & Boenisch, F. (2024). *Finding NeMo: Localizing Neurons Responsible For Memorization in Diffusion Models.* **Under Review at NeurIPS**. [*Arxiv Link*]
[2] **Struppek, L.**, Hintersdorf, D., & Kersting, K. (2024). *Be Careful What You Smooth For: Label Smoothing Can Be a Privacy Shield but Also a Catalyst for Model Inversion Attacks.* **ICLR**. [*Arxiv Link*]
[3] **Struppek, L.**, Hintersdorf, D., Friedrich, F., Brack, M., Schramowski, P., & Kersting, K. (2023). *Exploiting Cultural Biases via Homoglyphs in Text-to-Image Synthesis.* **JAIR**. [*Arxiv Link*]
[4] **Struppek, L.**, Hintersdorf, D., & Kersting, K. (2023). *Rickrolling the Artist: Injecting Backdoors into Text Encoders for Text-to-Image Synthesis.* **ICCV**. [*Arxiv Link*]
[5] **Struppek, L.**, Hintersdorf, D., Almeida, A., Adler, A., & Kersting, K. (2022). *Plug & Play Attacks: Towards Robust and Flexible Model Inversion Attacks.* **ICML**. [*Arxiv Link*]
[6] **Struppek, L.**, Hintersdorf, D., Neider, D., & Kersting, K. (2022). *Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash.* **FAccT**. [*Arxiv Link*]

Technical Skills and Interests

Languages: Python, Java
Developer Tools: Git, Docker
Frameworks: PyTorch, Scikit-learn, NumPy, Pandas, Matplotlib, Weights & Biases
Areas of Interest: Secure, Private & Trustworthy Machine Learning; Generative AI; Multimodal Systems

Positions of Responsibility

- **Board Member and Lecturer of EduRef** *2016–2020*
  Education for Refugees e.V., a Non-Profit Association Providing Educational Courses for Refugees
- **Supervisor of Programming Lectures & Seminars at KIT** *2016–2019*
  Responsible for 40 Teaching Assistants & 700 Students per Semester

Honors & Awards

- **Best Paper Award at ICLR Workshop** *2024*
- **Top Reviewer at NeurIPS** *2023*
- **Best Paper Award at IEEE Symposium on Security and Privacy Workshop** *2022*
- **Faculty Award of KIT Department of Economics and Management** *2022*
- **Winner of the Google Impact Challenge** *2018*
- **Deutschlandstipendium (Germany Scholarship)** *2017–2019*