

# Xun Wang

Ph.D. student, TUM & CISPA  
Saarbrücken, Germany

+49 15228041990 / +86 13834825901  
xun.wang@cispa.de | xun.wang@tum.de  
stephen016.github.io  
Google Scholar | GitHub | LinkedIn

**Research:** Trustworthy and efficient machine learning: privacy-preserving model adaptation and post-training (differential privacy, privacy auditing); model provenance and ownership (fingerprinting, IP protection); and trustworthy world models.

## EDUCATION

|                                                                                                                                                            |                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <b>Technical University of Munich (TUM) &amp; CISPA</b><br>Ph.D. in Computer Science (expected 2027), Saarbrücken, Germany. Advisor: Prof. Michael Backes. | Nov 2023 – Present  |
| <b>Technical University of Munich (TUM)</b><br>M.Sc. in Robotics, Cognition, Intelligence; High Distinction. Munich, Germany.                              | Oct 2020 – Aug 2023 |
| <b>Tongji University</b><br>B.Eng. in Vehicle Engineering. Shanghai, China.                                                                                | Sep 2015 – Jul 2020 |

## PUBLICATIONS

- [1] **Xun Wang**, Adam Dziedzic, Michael Backes, Franziska Boenisch. Auditing Privacy Leakage in Tabular Foundation Model Embeddings. **NeurIPS 2026**.
- [2] **Xun Wang**, Bihe Zhao, Michael Backes, Franziska Boenisch, Adam Dziedzic. AgentProv: Auditing Agentic LLM API Providers via Tool-use Policy Probes. **EMNLP 2026**.
- [3] Bartłomiej Marek, Lorenzo Rossi, Vincent Hanke, **Xun Wang**, Michael Backes, Franziska Boenisch, Adam Dziedzic. Benchmarking Empirical Privacy Protection for Adaptations of Large Language Models. **ICLR 2026 (Oral)**.
- [4] **Xun Wang**, Vincent Hanke, Jing Xu, Michael Backes, Franziska Boenisch, Adam Dziedzic. Frequency-Domain Model Fingerprinting for Image Autoregressive Models. **AIGOV@AAAI 2026 (Oral)**.
- [5] **Xun Wang**, Jing Xu, Franziska Boenisch, Michael Backes, Christopher A. Choquette-Choo, Adam Dziedzic. Efficient and Privacy-Preserving Soft Prompt Transfer for LLMs. **ICML 2025**.
- [6] Bihe Zhao, **Xun Wang**, Franziska Boenisch, Adam Dziedzic. Provenance Tracing for World Models: Was this Agent Trained in my World Model? **Under review**.
- [7] **Xun Wang**, John Rachwan, Stephan Günemann, Bertrand Charpentier. Structurally Prune Anything: Any Architecture, Any Framework, Any Time. **arXiv:2403.18955**, 2024. (Master's thesis)
- [8] Yunhui Wang, Meng Xiong, **Xun Wang**, Qile Li, Zhao Jiang, Xuezhe Wei, Haifeng Dai. Research on 11kW Wireless Charging System for Electric Vehicle Based on LCC-SP Topology and Current Doubler. **IEEE ECCE 2020**.

## RESEARCH EXPERIENCE

|                                                                                                               |                     |
|---------------------------------------------------------------------------------------------------------------|---------------------|
| <b>Doctoral Researcher, TUM &amp; CISPA</b><br>Saarbrücken, Germany.                                          | Nov 2023 – Present  |
| <b>Student Research Assistant, Technical University of Munich</b><br>Chair of Informatics 6, Munich, Germany. | Aug 2021 – Mar 2022 |

## HONORS & AWARDS

|                                                    |      |
|----------------------------------------------------|------|
| Oral Presentation, ICLR (top ~1.8% of submissions) | 2026 |
| Oral Presentation, AIGOV Workshop @ AAAI           | 2026 |
| <b>Gold Reviewer Award, ICLR</b>                   | 2025 |
| Graduated with High Distinction, M.Sc., TUM        | 2023 |

## TEACHING, SERVICE & SKILLS

|                                                                                             |                     |
|---------------------------------------------------------------------------------------------|---------------------|
| <b>Co-organizer</b> , First CISPA European Cybersecurity and AI Hackathon.                  |                     |
| <b>Teaching Assistant</b> , Machine Learning, TUM, Munich                                   | Oct 2021 – Mar 2022 |
| <b>AI-assisted development:</b> Proficient with Codex and Claude Code.                      |                     |
| <b>ML / Deep Learning:</b> PyTorch, Hugging Face Transformers, distributed training, Slurm. |                     |
| <b>Languages:</b> Chinese (native), English (fluent), German (B2).                          |                     |