CISPA
HELMHOLTZ-ZENTRUM FÜR INFORMATIONSSICHERHEIT

Fully-funded PhD positions in private and secure data-driven systems at CISPA, Saarbrücken, Germany

Dr. Ana-Maria Cretu has funded openings in her group at CISPA for PhD students to work on topics related to privacy, safety, and security in data-driven systems.

Topics. We study privacy, security, and user safety in general-purpose data systems, with a focus on generative AI systems, synthetic data, and anonymization. Our research tackles the question:

How can we design general-purpose data systems with provable privacy and safety?

To answer this question, we build tools to systematically reason about the trade-offs between general-purpose capabilities in these systems and their privacy and security requirements.

PhD projects. They are defined in close collaboration with the student, and could include e.g., evaluating capabilities of AI systems such as image generative AI [1] and client-side scanning systems [2,3], or designing tools to measure and enhance the privacy and utility of privacy-enhancing technologies like synthetic data [4], query-based systems [5,6], and anonymization [7]. They will typically include a mix of theoretical work and empirical evaluation aimed to generate significant real-world impact. Our work is published in top-tier security conferences and journals such as ACM CCS, USENIX Security, IEEE SP, and Nature Communications as well as top-tier machine learning conferences (EMNLP, ACL).

PhD conditions. A PhD at CISPA normally takes 3-4 years and is fully-funded with excellent working conditions. The start-date is flexible. PhD researchers at CISPA are full-time employees paid according to the TVöD (German Federal Employment Agreement), up to the E13 level. Salaries start at around €4,000 (gross/month). CISPA offers 30 days paid time off and a pension scheme, as well as opportunities for development and growth from language classes, research support to extracurricular and social activities, and support by the onboarding team.

Pre-requisites. Bachelor's or Master's degree (e.g., MSc, MEng) in Computer Science, Statistics, Mathematics, Physics, or Electrical Engineering. The student should have an excellent academic record or outstanding relevant research or practical experience, English proficiency, a rigorous and systematic approach to research, and a strong interest in security and machine learning.

About CISPA. The CISPA Helmholtz Center for Information Security is the world-leading institution in computer security research. CISPA employs more than 40 faculty working on all areas of information security such as cryptography, trustworthy machine learning, empirical security, etc., fostering a uniquely rich security-oriented collaborative environment. CISPA offers excellent working conditions for PhD students, such as highly competitive salaries and paid leave days as well as generous funding and excellent scientific support.

How to apply. Prospective candidates are encouraged to email Ana-Maria Cretu at cretu@cispa.de with a CV, a transcript of academic records for all degrees, and 2-3 references.