

The Department of Computer Science (of the Faculty of Mathematics, Computer Science and Physics) at the University of Innsbruck, Austria, seeks to fill the position of a research assistant

PhD Student (University Assistant)

in the area of

Cryptography

as soon as possible.

Who We Are The Security & Privacy research group at the University of Innsbruck is dedicated to advancing knowledge and understanding in the fields of information security and privacy. Our research covers a range of topics, including cryptography, privacy-enhancing technologies (PET), digital currencies. We collaborate with other leading institutions and organizations to ensure the protection of fundamental human rights in the digital world. We are committed to conducting high-quality research and providing exceptional education in these crucial areas. For more information please visit our group's website:

<https://informationsecurity.uibk.ac.at/>.

Who We Are Looking For We are growing our international team and looking for a paid research assistant with a degree in computer science, mathematics, or related areas. Candidates should be interested in pursuing a PhD by doing excellent research in the area of security & privacy and learning and exploring innovative methods and solutions. Besides the ability to work independently and collaboratively, candidates should be committed to challenging the status quo as a researcher. Leading motivated undergraduate and graduate students is another enjoyable part of our work and an opportunity for your personal growth as a teacher or supervisor.

What We Offer Successful candidate will benefit from working in a supportive, welcoming, and dedicated environment that appreciates and promotes interdisciplinary research. They will also benefit from a broad research network and established partnerships with academics, industry, and governmental institutions working on related topics around the globe. Successful applicant will work with Dr. Arnab Roy on advancing research in cryptography for secure & private computation.

More specifically successful applicant will work on

- Secure and efficient construction of cryptographic functions for ZK proof systems, multiparty computation protocol and homomorphic encryptions;
- Cryptanalysis techniques for above mentioned cryptographic functions;
- Implementation of cryptographic functions using suitable protocol frameworks or platforms.

Located in the heart of the Alps, Innsbruck offers a diverse variety of exciting sports activities and cultural experience. The members of our group regularly visit mountain huts, hiking trails, and ski slopes to seek for inspiration and brainstorm in the nature.

What We Require Candidates for this position are expected to bring the skills, motivation, and perseverance necessary to conduct interdisciplinary research and successfully complete a PhD.

- Master's degree or equivalent in mathematics, computer science or a related field;
- Ability to conduct independent research; motivation to learn new methods and topics;
- Willingness to publish and present research outputs at international venues;
- Willingness to assist in teaching, event support and administrative activities;
- Good knowledge of basic Algebra and willingness to learn advanced topics;
- Social competencies, communication and teamwork skills, proactive attitude;
- Proficiency (written and oral) in English.
- Prior research experience (e.g. master's thesis, publication) in Mathematics (algebra/number theory) or Computer Science is an advantage.
- Experience in C/C++ or Python.. Experience in \LaTeX and Rust is a plus..

How to Apply The application must be submitted in English and must contain:

- your CV with a description of the academic (and professional) career;
- a letter of motivation;
- certificates and academic transcripts of records.

The minimum gross salary (stipulated by collective agreement) for 20 hours per week amounts to €1,529 per month (14 times). The salary will be increased to €2,293 for 30 hours per week once the dissertation agreement has been signed and sent to the Personnel Department. The salary will be higher if you have worked in a similar position before. Furthermore, the university has numerous attractive offers (<https://www.uibk.ac.at/universitaet/zusatzleistungen/>).

The University of Innsbruck emphasizes equal opportunities and diversity in its personnel policy.

The University of Innsbruck strives to increase the proportion of its female employees, especially in leadership positions, and therefore explicitly invites women to apply. In the case of equivalent qualifications, female applicants will be given preference.

We look forward to receiving your online application (Chiffre MIP 13843) until

09 November 2023.

The legally binding text in German is available at:

https://lfuonline.uibk.ac.at/public/karriereportal.details?asg_id_in=13843.