Postdoctoral

Ecole/Institution/Société:
Aalto University School, **Finland / Helsinki**

Discipline:
Applied Mathematics, Computational Engineering

Type d'emploi::
Full-time

Date de publication:
2022-04-27

Personne à contacter:
If you wish to apply for this position, please specify that you saw it on AKATECH.tech

Postdoctoral Researcher in Mathematics or Computer Science: Lattice-Based Cryptography

Aalto University is a community of bold thinkers, where science and art meet technology and business. We are committed to identifying and solving grand societal challenges and building an innovative future. Aalto has six schools with nearly 11 000 students and a staff of more than 4000, of which 400 are professors. Our main campus is located in Espoo, Finland.

Diversity is part of who we are, and we actively work to ensure our community's diversity and inclusiveness in the future as well. This is why we warmly encourage qualified candidates from all backgrounds to join our community.

The Department of Mathematics and Systems Analysis (http://math.aalto.fi/en/) is seeking a

Postdoctoral Researcher in Mathematics or Computer Science: Lattice-Based Cryptography

We are looking for a post-doctoral researcher in the area of lattice-based cryptography. Possible research topics include:

- Cryptanalysis of lattice problems
- Side-channel analysis of implementations of lattice-based cryptography
- Lattice-based cryptographic protocols
- Construction of new candidate structures suitable for, e.g., the ring learning with errors (RLWE) problem and its variants.
- Research experience in cryptography is essential. Additionally, background in algebraic number theory, probability theory, complexity theory and/or machine learning are useful. For a cryptographer, we expect that the candidate has published in IACR conferences, established theoretical computer science venues (STOC/FOCS/APPROX-RANDOM/SODA/PODC) or IT security venues (CCS/S&P/Usenix). The applicant is expected to hold a PhD degree in mathematics or computer science. A research level proficiency in English, both writing and speaking, is expected.

We offer advising related to both algebraic lattices (Camilla Hollanti) and cryptography (Chris Brzuska). Our group offers a diverse, international, and open research environment. We expect the candidate to significantly shape the research questions which we investigate together as well as to pursue their own research with their existing research network. Additionally, the candidate can benefit from our extensive academic and industrial networks.

Formally, the position will be supervised by Camilla Hollanti and be part of the Algebra, Number Theory, and Applications (ANTA) Group. ANTA is part of the Department of Mathematics and Systems Analysis https://math.aalto.fi/en/ which hosts several strong research groups, including Chris Brzuska Group. Chris Brzuska has a double appointment at the Department of Computer Science (https://www.aalto.fi/en/department-of-computer-science), which is home to several strong research groups in machine learning and complex systems as well as theoretical computer science.

Your application should include the following documents:

- Statement of purpose (describe your motivation, mathematics and other relevant skills, scientific interests and career goals, and mention your preferred starting date).
- CV.
- University transcripts (with clear explanation on the grading scale).
- PhD certificate (or estimated graduation date if not yet finished).
- Names and contact details (positions, emails and phone numbers) of two references
- For additional information on the position, please contact Camilla Hollanti or Chris Brzuska (both eMails: firstname.lastname@aalto.fi). For submission related queries, contact Johanna Glader (firstname.lastname@aalto.fi).

*Please note: Aalto University's employees and visitors should apply for the position via our internal system Workday -> career - find jobs, (not external aalto.fi webpage on open positions) by using their existing Workday user account.

Aalto University reserves the right for justified reasons to leave the position open, to extend the application period, and to consider candidates who have not submitted applications during the application period.

Finland is known for high quality of life, great work-life balance, clean nature, and family-friendly policies such as affordable high-quality daycare and free schools. Helsinki is a vibrant international city with a metropolitan area population of over 1.1 million people. Aalto University is an equal opportunity employer dedicated to attracting, retaining and developing our people regardless of gender identity, ethnicity, disability, and age. We encourage applications from all suitably qualified individuals from all sectors of the community.

More about Aalto University:

- Aalto.fi
- twitter.com/aaltouniversity
- facebook.com/aaltouniversity
- instagram.com/aaltouniversity

Job details

Title: Postdoctoral Researcher in Mathematics or Computer Science: Lattice-Based Cryptography

Employer: Aalto University

Location: Lämpömiehenkuja 2 Helsinki, Finland

Job type: Postdoc

Field: Applied Mathematics, Computational Mathematics, Computational Sciences, Informatics

Personne à contacter:
If you wish to apply for this position, please specify that you saw it on AKATECH.tech