

Postdoc/PhD Student in Applied Multi-Party Computation

The Computer Security and Industrial Cryptography (COSIC) group belongs to the Electrical Engineering Department at the KU Leuven. The COSIC team has about 90 researchers including 7 professors, 8 researcher managers/experts, 20 postdoctoral researchers, 50 PhD students, 5 visitors and 6 members of support staff.

The COSIC research group provides a broad expertise in digital security and strives for innovative security solutions. Our research is applied in a broad range of application domains, such as electronic payments, identity cards, e-voting, protection of e-documents, smart meters and smart grid, telematics for the automobile industry and trusted systems. Our research focus lays in the design, evaluation and implementation of cryptographic algorithms and protocols, the development of security architectures for information and communication systems, the development of security mechanisms for embedded systems and the design and analysis of privacy preserving systems. The group has as goal to cover the whole range from mathematical theory towards industrial applications.

COSIC is looking for motivated researchers who fit into the following profile:

Postdoc/PhD Student to work on Applied Multi-Party Computation

Job description

We are looking for people to work on **applied multi-party computation**. Experience with network programming, security protocols, or compiler technology would be a great advantage. You will be collaborating closely with researchers to improve the quality and performance of an open source project <https://github.com/KULeuven-COSIC/SCALE-MAMBA>.

We are particularly interested in applicants who are interested in working on building and designing languages to describe secure computation problems, and then building compilers to turn these algorithmic descriptions into running code.

Specific skills required

Strong background in mathematics/computer science and/or cryptography. PhD applicants we would prefer to have experience in C or C++. For Postdoc researchers experience in practical aspects of secure computation or experience in compiler technology is a must.

How to apply

Visit <https://www.esat.kuleuven.be/cosic/vacancies/>