

**PhD/PostDoc positions in secure computation
(FWO Odysseus, DARPA RACE, IARPA Hector)**

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, 20 postdoctoral researchers, 50 PhD students, 5 visitors and 5 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, intelligent home appliances, 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:

PhD candidate or a **PostDoc researcher** to work on various aspects of secure computation.

Job Description: We have a number of positions in the area of secure computation based on multi-party computation (MPC) and Homomorphic Encryption. The positions are funded by three projects; an FWO grant under the Odysseus programme, a DARPA grant under the RACE programme and an IARPA grant under the Hector programme. The goal of the research is to develop new methods for efficient MPC, methods to apply MPC to large numbers of parties, methods to build automated tools to support development of applications based on MPC and FHE, as well as innovative new MPC solutions which solve real world problems. We are looking for applicants who can work on practice inspired theoretical work in MPC, applicants who can work on implementation research in MPC and FHE, applicants with previous experience in programming language research, as well as applicants working in theoretical aspects of the MPC and FHE.

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 theoretical or practical aspects of secure computation is a must.

How to apply: Send following documents (in pdf) to *jobs-cosic@esat.kuleuven.be*

- Curriculum Vitae.
- Motivation letter.
- List of publications.
- Relevant research experience.
- Study curriculum with rankings.
- English proficiency.
- PDF of diploma and transcripts (translation if the original is not in Dutch, English, French or German).
- Research proposal (1 page) describing which research questions you would like to work on.
- Names (and e-mail) of 2 reference persons and the nature of contact with them .