

Postdoc/PhD Student in Protocol Design and Analysis

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 a 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 Protocol Design and Analysis

Job description

We are looking for people to work on the **design and analysis of cryptographic protocols**. We are interested in applicants who are interested in a diverse range of protocols types; from applied protocols such as TLS, IPSec, etc through to more specific protocols such as distance-bounding and OT. We are particularly interested in people with experience, or interest, in using automated tools to analyse such protocols. Our goal is to analyse a wide range of practical protocols using a number of tools and techniques; from pen-and-paper analysis via game-based or UC models, to automated detection of bugs or generation of security proofs via tools like CryptoVerify or EasyCrypt.

Specific skills required

Strong background in mathematics/computer science and/or cryptography. For Postdoc researchers we expect experience in computational protocol analysis (games based/UC) and/or the usage of formal tools (such as CryptoVerif or EasyCrypt) is a must.

How to apply

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