PhD/postdoc position in white-box cryptography

The Computer Security and Industrial Cryptography (COSIC) group belongs to the Electrical Engineering Department at the KU Leuven. The COSIC team has about 70 researchers including 5 professors, 26 postdoctoral researchers, 43 PhD students, 2 visitors and 6 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 focuses on 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 **white-box cryptography**

White-box cryptography implementations are software implementations of cryptographic functions that hide the secret key against an opponent with full access to the software. These implementations are widely used for content and software protection. All existing published methods to white-box standardized ciphers have been broken.

Job description
The applicant will participate in the High Impact Initiative on Distributed Trust of Imec – KU Leuven. The student will need to develop novel approaches to the design of white-box ciphers and the design of white-boxing methods for existing ciphers; software tools to evaluate the strength of white-box solutions as well as a software tools to transform white-box code.

Specific skills required
Strong background in mathematics and preferably experience with implementing advanced mathematical structures.

How to apply

Send the following documents (in pdf) to jobs-cosic@esat.kuleuven.be by January 31st, 2017.

- 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