**PhD Position: Cryptography secured against side-channel attacks**

**COSIC, KU Leuven**
The Computer Security and Industrial Cryptography group (COSIC) currently has over 55 researchers. The research work of COSIC covers a broad span that varies from mathematical foundations over algorithms and protocols towards efficient and secure implementations in hardware and software. This research of COSIC has led to important successes in the area of cryptanalysis and design; notable successes are the selection of the Rijndael algorithm as the US Advanced Encryption Standard (AES), which is a worldwide standard today and the development of efficient algorithms to count points on elliptic curves.

**Project Description**
It is not known how to design cryptographic algorithms that remain secure if the attacker has also access to the intermediate results. Therefore, the current research concentrates on implementation techniques that ensure that the intermediate results of the cryptographic algorithm are statistically independent of the secret key.

A new method to construct provably secure against side-channel attacks implementations (called Threshold Implementation) has been proposed by researchers from COSIC. The approach is based on secret sharing and multi-party computation methods. Proof-of-concept implementations have been proposed already for several ciphers including Present and AES. We can prove security against attacks that are based on correlating a secret variable to the expected values of the power consumption or any other side-channel of a device.

The project is funded by various sources: Research Foundation – Flanders (FWO), KU Leuven Research Fund and NIST. We also collaborate with IMEC (www.imec.be), Belgium. **Contact:** {svetla.nikova,vincent.rijmen}@esat.kuleuven.be, liesbet.vanderperre@imec.be

**Research**
Currently, we are investigating how we can achieve security against more advanced attacks. The research combines mathematical methods and insights with statistical methods and circuit design techniques. We are also interested to learn how our approach will be affected by the use of future technologies, which can further scale down cost and power while allowing more signal processing complexity.

The student will research issues related to one or more of the following work-packages:

1. Extending the mathematical framework of the Threshold Implementation approach,
2. Assessing real-life effects that occur in modern CMOS technologies, when countermeasures are applied,
3. Determining the overhead introduced by our protection measures and to evaluate its cost and effectiveness by doing experiments in an emerging technology.

The exact task description will be agreed upon with the student during or after the hiring process.

The student will work closely together with several other PhD students, and postdoctoral fellows. The student has to be able and willing to work in team.

**Student profile**
The candidates should hold a master degree in Engineering, Mathematics or Computer Science, very good knowledge in C/C++ and Verilog/VHDL. Preferably to have passed courses in Cryptography and/or Computer Security.
Selected References