CELSA

Central Europe Leuven Strategic Alliance

CELSA - Collaborative research project - Application form - COVER PAGE

1. Identification of the principal investigator – co-ordinator
Full name: Nele Mentens
Faculty/Department: Faculty of Engineering Technology, Technology Cluster ESAT
Research unit within Faculty/Department: Embedded Systems & Security
Address: Wetenschapspark 21, 3590 Diepenbeek
University: KU Leuven
Tel: +3211180920
Fax:
Email: nele.mentens@kuleuven.be
Signature[1]:

2. Identification of the second investigator
Full name: Martin Novotný
Faculty/Department: Faculty of Information Technology, Department of Digital Design
Research unit within Faculty/Department:
Address: Thákurova 9, 160 00 Praha 6
University: CTU in Prague
Tel: +420-22435-9832
Fax :
email : martin.novotny@fit.cvut.cz
Signature[1]:

3. Identification of third and fourth co-investigator(s) (if applicable) Expand table if more than four research units are involved.	
Third co-investigator	**Fourth co-investigator**
Full name:	Full name:
Faculty/Department:	Faculty/Department:
Research unit within Faculty/Department:	Research unit within Faculty/Department:
Address:	Address:
University:	University:
Tel:	Tel:
Fax:	Fax:
email:	email:
Signature[1]:	Signature[1]:

[1] Faxed signatures will be accepted.

3. Non confidential and public friendly summary (max. 2000 characters)

Project title:

DRASTIC: Dynamically Reconfigurable Architectures for Side-channel analysis protecTIon of Cryptographic implementations

Summary:

The Internet of Things (IoT) is increasingly becoming part of our everyday life. Therefore, electronic IoT devices need to be carefully designed, taking into account data security and privacy. Putting in place security and privacy measures should introduce a minimal overhead in the system's power/energy consumption, cost and operational delay. Additionally, since IoT devices are everywhere, attackers can be in the vicinity of the device, which stresses the need for protection against side-channel analysis (SCA) attacks. These attacks exploit the use of side-channels, which are information channels that are unintentionally present in electronic devices and which potentially leak secret information. Examples are the power consumption, the electromagnetic radiation and the timing behaviour of the electronic device. In both academia and industry, SCA countermeasures are being developed and deployed. However, as SCA attacks become more and more sophisticated, continuously evolving countermeasures are necessary to protect the electronic devices of the future.

This project proposes the use of dynamic hardware reconfiguration as a countermeasure against one of the most exploited types of SCA attacks, namely power analysis attacks. The goal is to randomly change the hardware circuit without altering the input-output behaviour of the chip. Since power analysis attacks are strongly based on the knowledge of the circuit, this is a very promising countermeasure. Another advantage is that dynamic hardware reconfiguration can be used as an add-on to other countermeasures. The project focuses on dynamic hardware reconfiguration on FPGAs (field-programmable gate arrays). It will result in proof-of-concept implementations that will be evaluated for power analysis attack resistance. The experimental results are crucial for the definition of a European project proposal that develops an automated tool flow and industry-driven use cases to show the effectiveness of the approach.

4. List 5 key words

Internet of Things, cryptography, embedded security, FPGA, side-channel analysis, dynamic hardware reconfiguration