HECTOR

Hardware enabled crypto and randomness

Message from the Coordinator

Security has become a critical requirement for most applications. **Robust security** typically **requires strong hardware** foundations. HECTOR's mission was to **bridge the gap** between the mathematical heaven of theoretically secure cryptographic algorithms and the challenges when it comes to implementing them securely and efficiently into hardware. The project focused on how to **improve** the **hardware efficiency and robustness of 3 elementary security building blocks**, namely **crypto algorithms, random numbers generators**, and **physically unclonable functions (PUFs)**, as well as opportunities to optimize their interactions.

For **true random number generators (TRNGs)**, the requirement is to fulfil demanding security requirements such as specified by the **AIS20/31 standard** in order to guarantee the generation of enough entropy, and/or detect and report when this is no longer the case. Besides **designing hardware-efficient TRNG cell(s)**, the main ambition was to propose a process allowing to meet the requirements while minimizing the necessary expertise, design-iterations, and efforts.

Compared to TRNGs, so far there is no AIS20/31-like framework for PUFs. The objective was therefore to research if such an approach could be proposed.

Newsletter / August 2018 - Issue 5

Consortium
9 partners (6 countries)

Project Coordinator
Dr. Klaus-Michael KOCH
coordination@hector-project.eu

Scientific Lead
Prof. Ingrid Verbauwhede
ingrid.verbauwhede@esat.kuleuven.be

Technical Lead
Bernard Kasser
bernard.kasser@st.com

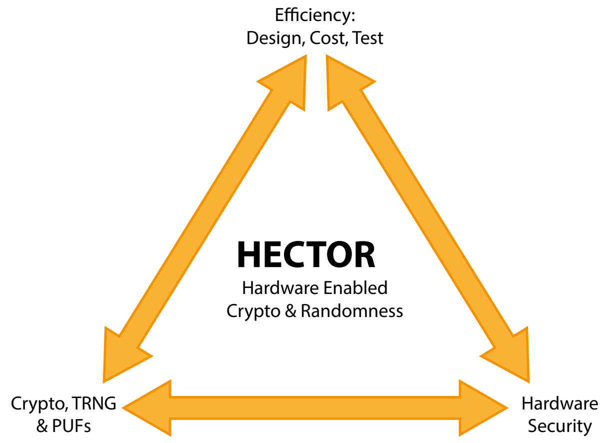
Project number:	**644052**
Project website:	**www.hector-project.eu**
Project start:	**1st March, 2015**
Duration:	**3 years**
Total cost:	**EUR 4,494.087,50**
EC contribution:	**EUR 4,494.087,50**

Main objectives achieved

From a socio-economic point of view, HECTOR enabled a stronger European knowledge integration through collaboration among key security actors. Additionally, the following main objectives have been fully achieved. TRNG (true random number generators) designs (secure-by-design) with provable entropy guarantees and robustness to physical attacks were proposed successfully. This paves the way for more robust products and lower cost security certification.

Furthermore, this allows to increase the security of semiconductor components and the confidence level for products based on these. The benefits are already materializing for the most "technology-ready" HECTOR primitive with the adoption of HECTOR's PLL-TRNG design approach within 2 automotive components from partner STMicroelectronics.

A complete set of tools including reference design architectures, stochastic models, embedded tests, post-processing algorithms including security proofs and a standard workflow that will ease the security certification process, has been produced successfully. The robustness of the proposed TRNG against active and passive attacks could also be verified.



In deliverable D4.2 three demonstrators including key performance indicators have been specified and in the public deliverable D4.3 a vulnerability analysis was performed. The demonstrators aim to illustrate how the design and the approaches of HECTOR primitives (TRNG, PUF and AE) are suitable to deal with relevant security use cases. It helped generating business opportunities for partners who will be using HECTOR-generated technologies and know-how in products specifically targeting security-critical applications for European customers with use cases similar to HECTOR demonstrators 2 and 3.

Demonstrator 1: Standalone, high performance secure random number generator device.

The outcome of the vulnerability analysis showed that there are no exploitable attack scenarios for Demonstrator 1.

Several evaluation work items were done and show that the TRNGs in the device provide sufficient entropy in the raw random numbers over a large temperature range. A webservice to request and generate an arbitrary amount of true random data was established and is accessible via: https://trng.technikon.com

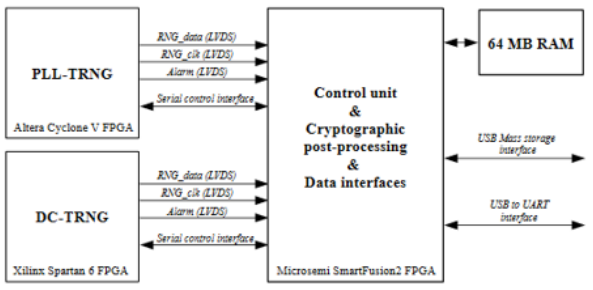


Figure 1: Hardware Platform of Demonstrator 1

Demonstrator 2: A portable device aimed at protecting data at rest.

For Demonstrator 2 the vulnerability analysis showed that the high entropy offered by the pass-phrase does not allow feasible attack scenarios on the secured data at rest.

Attacking a live device is impractical because it requires chip-level attacks while the user is entering the pass-phrase and the PUF response is being reconstructed. Chip-level attacks are beyond the attack potential of the envisioned attackers.

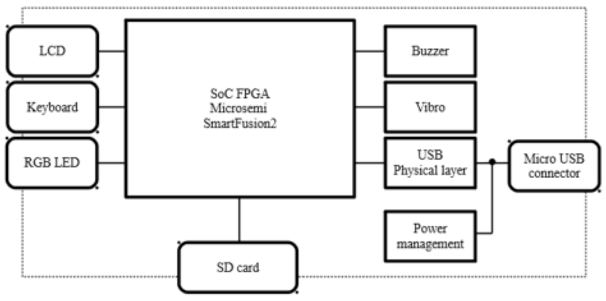


Figure 2: Hardware Platform of Demonstrator 2

Demonstrator 3: To protect data in motion between secure messaging devices.

Similar as for Demonstrator 2, attacking live communication requires chip-level attacks while the user pass-phrase is being entered and the PUF response is being reconstructed.

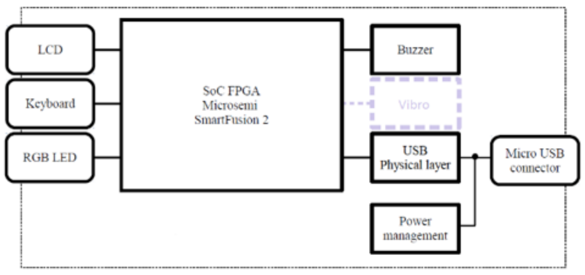
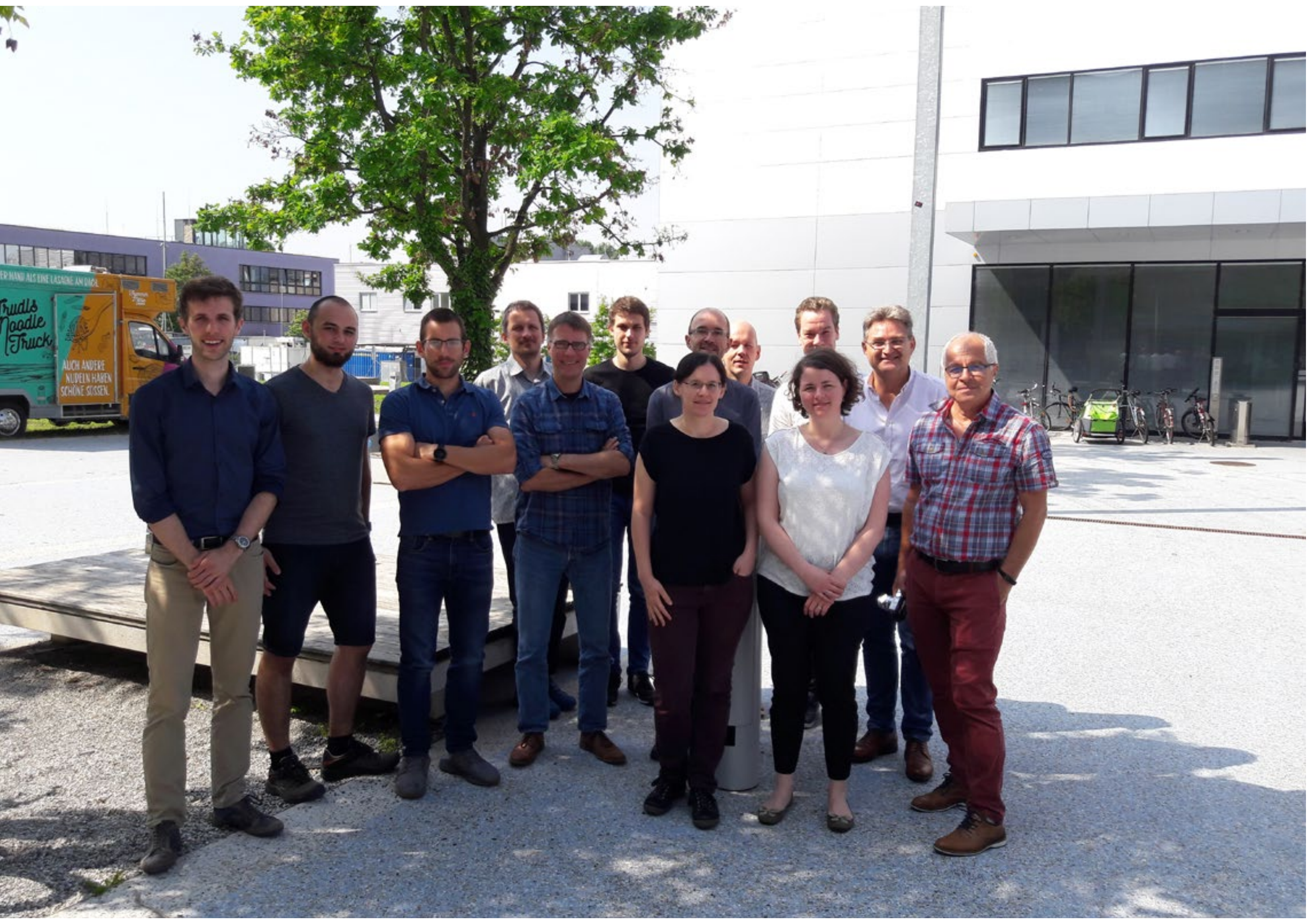


Figure 3:Hardware Platform of Demonstrator 3

Technical Meeting in Graz



From 29th – 30th May the **HECTOR technical meeting** took place at the University of Technology in Graz, Austria.

The first day was dedicated to prepare the **final review meeting** in **September in Amsterdam, The Netherlands**. The work package leaders presented the results and achievements as well as the ongoing work in the individual work packages.

On the second day the status and the ongoing work of the Deliverables D2.4, D5.4 and D5.5 were presented.

Upcoming Events

HECTOR Third and Final Review Meeting -
11th September 2018
@Amsterdam, The Netherlands

Conference on Cryptographic Hardware and Embedded Systems 2018 (CHES 2018) -
9th - 12th September 2018
@Amsterdam, The Netherlands

CARDIS Smart Card Research and Advanced Application Conference -
12th - 14th November 2018
@Montpelier, France

All project results **(scientific publications and deliverables)** are accessible on our project website: **hector-project.eu**

Submitted Public Deliverables

D2.2 ASIC and FPGA Designs

D3.1 Report on the Efficient Implementations of Crypto Algorithms and Builings Blocks and on Cost and Benefits of Countermeasures Against Physcal Attacks

D3.3 Report on the Security Evaluation of Cryptographic Algorithms and Countermeasures when non-Ideal Hardware Building Blocks are Used

D4.1 Demonstrator Specification

D4.2 Demonstrator platforms accompanying report

D4.3 Security Evaluation of the HECTOR Demonstrators

Follow **HECTOR** on:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052.