Newsletter

HECTOR

May 2017 - Issue 3

HECTOR

Activities within the 2nd Project Period

The first six months of the 2nd project period were very active. The TERO PUF was implemented in the Microsemi SmartFusion2 FPGA. Furthermore, the PUF is ready to be integrated in two of three demonstrators. In addition to that, the PLL-TRNG design was optimized for FPGA implementations in all three demonstrators and the ASIC design was submitted. Besides that, Task 4.2 "Integration of Hardware Modules" and Task 4.3 "Software Layer &User Interface" are progressing as well, since all building blocks integrated on the target hardware platform are functional. Apart from the technical progress, the project was also active on the dissemination and the management side. During this reporting period, several publications have been accepted for presentations at conferences. Moreover, additional research output, such as the ASCON, KETJE and AES implementation as well as training material have been made publicly available on the project website. The first periodic report could be finalized and a successful first review meeting took place in Leuven in October 2016.

IN THIS ISSUE

Technical Meeting in Graz

In March 2017, TU Graz hosted a technical face-to-face meeting of the HECTOR project. The three days were packed with talks, presentations and exchange of information related to ASIC manufacturing and TRNG implementation. The most important discussion point was all about the three demonstrators. Single building blocks have been reviewed and the status and challenges of integration work have been discussed. Brightsight gave an interesting presentation about attacks on TRNGs and PUFs. An administrative slot focused on the achievement of the upcoming milestones.

HECTOR Publications 2017

"Practical Key Recovery Attack on MANTIS-5"; TOSC-FSE-2017; C. Dobraunig, M. Eichlseder, D. Kales, F. Mendel

"An Efficient Side-Channel Protected AES Implementation with Arbitrary Protection Order"; CT-RSA 2017; H. Gross, S. Mangard, T. Korak

"Complete activation scheme for IP design protection"; HOST 2017; B. Colombier, U. Mureddu, M. Laban, O. Petura, L. Bossuet, V. Fischer

"Key Reconciliation Protocols for Error Correction of Silicon PUF Responses"; IEEE Transactions on Information Forensics and Security 2017; B. Colombier, L. Bossuet, D. Hély, V. Fischer

"ISAP -- Towards Side-Channel Secure Authenticated Encryption"; TOSC-FSE-2017; C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, T. Unterluggauer

"Symbolic Analysis of Higher-Order Side Channel Countermeasures"; IEEE Transactions on Computers 2017; E. Bisi, F. Melzani, V. Zaccaria

"Physically Unclonable Function using CMOS Breakdown Position"; 54th International Reliability Physics Symposium - IRPS 2017; K.-H. Chuang, E. Bury, R. Degraeve, B. Kaczer, G. Groeseneken, I. Verbauwhede, D. Linten

Start Date: 1st March 2015
End Date: 28th February 2018
Duration: 36 months
Project Reference: 644052
Project Costs & Funding: € 4.494.087,50

Project Website: www.hector-project.eu

Consortium: 9 partners (6 countries)

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

Technical Leader: Bernard Kasser
bernard.kasser@st.com

Scientific Leader: Prof. Ingrid Verbauwhede
ingrid.verbauwhede@esat.kuleuven.be

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

https://twitter.com/HECTOR_H2020

Newsletter

HECTOR HECTOR

May 2017 - Issue 3

Presentation of the three demonstrators

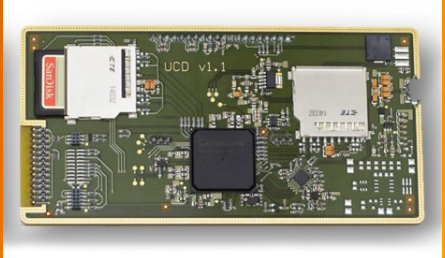
Demonstrator 1: Stand alone TRNG

Demonstrator 1 is a physical true random generator including cryptographic post-processing, which is aimed at generation of random bit streams achieving security level PTG.3, as defined in AIS 20/31. The generation of random numbers is provided as a security service for the user.

Two kinds of sources of randomness and associated random number generators exploiting these sources are demonstrated to be compliant with AIS 20/31 in the two operational modes of the device: (i) **PLL-based TRNG, (ii) Delay chain-based TRNG**. The aim of Demonstrator 1 is to show that the proposed TRNG designs can be successfully applied in high-end real-world data security applications, in which a secure and robust TRNG is an essential construction block. The proposed demonstrator could be used as a stand-alone security peripheral - the source of high quality random numbers - in high-performance data servers and communication systems.

Demonstrator 2: Secure USB stick

Commonly known USB storage devices are popular means of data storage, back-up and transfer. Such a device may contain sensitive personal information and/or company assets in digital form, e.g. bank statements, legal documents, commercial treaties, sales and billing documents, source codes, technical documentation or other intellectual property. The risk for the information to be compromised is high when commuting, travelling, or just leaving the drive unattended in a car or a hotel room. Demonstrator 2 is a secure portable USB storage: a personal, single-user device that protects the data stored on it while being at rest. It requires the user to authenticate before allowing access to the data and is powered from the USB bus without the need of an external power source.



- A **TRNG compliant with AIS 20/31 PTG.2** introduces the online test which immediately detects and stops any defect in random data generation.
- **Authenticated encryption** ensures confidentiality and integrity of the data in a single operation.
- **Physically unclonable function** binds the encrypted data to the particular piece of hardware.

The combination and the efficient implementation of all aforementioned principles are brand new, as it is the impact in the real world.

Demonstrator 3: Secure messaging device

Enabling the ability for users to communicate securely remains today one of the major use cases of cryptography. Popular messaging applications such as Facebook Messenger, Whatsapp or Apple iMessage are able to handle traffic load of several billions of messages everyday. When one adds to that the volume of data sent via text message or emails, the importance of protecting those communications becomes obvious.

Within the framework of the HECTOR project, the usage of the PUF coupled with user's passphrase can be used as a strong two factor authentication protocol that prevents an outsider from communicating with a peer even if the whole device is compromised. The use of sponge based primitives dispenses with using ad hoc constructions to guarantee not only that messages are confidential and authenticated but also that the whole stream of messages hasn't been tampered with (replay-protection, reorder-protection). The aim of Demonstrator 3 is to showcase that the cryptographic primitives developed within HECTOR can successfully be applied in high-end real-world data security applications in which user and device authentication must be strong and confidential messages are both encrypted and authenticated.

Start Date: 1st March 2015
End Date: 28th February 2018
Duration: 36 months
Project Reference: 644052
Project Costs & Funding: € 4.494.087,50

Project Website: www.hector-project.eu

Consortium: 9 partners (6 countries)

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

Technical Leader: Bernard Kasser
bernard.kasser@st.com

Scientific Leader: Prof. Ingrid Verbauwhede
ingrid.verbauwhede@esat.kuleuven.be

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

https://twitter.com/HECTOR_H2020