Newsletter

September 2015 - Issue 1

HECTOR

MAIN PROJECT INFORMATION

HECTOR aims to **close the gap between the mathematical heaven of cryptographic algorithms** and their efficient, secure and robust hardware implementations. The consortium aims for a stronger European knowledge integration through collaboration among key complementary European security technology and value chain actors, in order to fully unleash and leverage Europe's security innovation, competitiveness, and leadership potential.

A **single flipped bit or a weak random number generator** can cause secure systems to fail. Therefore, the main motivation of this project is to **bridge basic algorithmic approaches with hardware-level security implementations**. It requires integrating secure cryptographic primitives such as random number generators (**RNGs**) and physically uncloneable functions (**PUFs**), together with physical attack countermeasures. The goal is to study, design and implement RNGs and PUFs with demonstrable entropy guarantees and quality metrics. This includes **on-the-fly entropy testing and physical attacks evaluations**, which will enable more secure systems and easier certification.

IN THIS ISSUE

MESSAGE FROM THE COORDINATOR

The intention of this Newsletter is to open a new communication channel in order to provide news on the project progress and to discuss ongoing topics relevant to HECTOR for internal and external project partners, stakeholders and all other interested bodies. For more detailed information about and around the project we warmly invite you to have a look on our project website, which is constantly kept up-to-date with the latest project related news: www.hector-project.eu.

The project has successfully started with the Kick-Off meeting in March 2015 and since then the project has been in its initial stages of formation. The HECTOR project has a well-balanced and focused consortium - comprising 9 project partners from 6 different European countries - including experts from large and SME companies, academy and certification labs with a track record on cryptographic algorithm development, RNG design, side-channel and fault attach protection, as well as efficient hardware or embedded software implementations.

HECTOR PUBLICATIONS

- **A Physical Approach for Stochastic Modeling of TERO-based TRNG** (Best Paper Award Winner) in Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2015; P. Haddad, V. Fischer, F. Bernard, J. Nicolai
- **Forgery and Subkey Recovery on CAESAR candidate iFeed** in 22nd International Conference on Selected Areas in Cryptography, SAC 2015; KU Leuven
- **On the Impact of Known-Key Attacks on Hash Functions** in ASIACRYPT, 2015; B. Mennink, B. Preneel

UPCOMING EVENTS

- **CHES 2015 - Cryptographic Hardware and Embedded Systems**
  13th - 16th September, 2015; Saint-Malo / France
- **1st HECTOR AB/GA Meeting**
  3rd - 4th November, 2015; Gennevilliers / France
- **1st HECTOR Review Meeting**
  10th December, 2015; Brussels / Belgium

***Start Date*:**	1 March 2015	***Consortium*:**	9 partners (6 countries)
***End Date*:**	28 February 2018	***Project Coordinator*:**	Dr. Klaus-Michael Koch coordination@hector-project.eu
***Duration*:**	36 months		
***Project Reference*:**	644052	***Technical Leader*:**	Bernard Kasser bernard.kasser@st.com
***Project Costs & Funding*:**	€ 4.494.087,50		
		***Scientific Leader*:**	Prof. Ingrid Verbauwhede ingrid.verbauwhede@esat.kuleuven.be

***Project Website*:**
www.hector-project.eu

https://twitter.com/HECTOR_H2020

Newsletter

September 2015 - Issue 1

HECTOR

TECHNICAL INFORMATION

The work performed in the framework of this project is organized in six different work packages tailor-made to achieve the maximum of efficiency and output quality.

WP1 “Requirements Specification” intends to derive industry-driven requirements and specifications for the building blocks in WP2, WP3 and the demonstrator in WP4.

WP2 “RNGs and PUFs” contains the core technology of the HECTOR project and will include the design and selection of suitable TRNG and PUF principles. Furthermore, it will include deriving stochastic models, the implementation and finally the evaluation as well as advanced testing of the designed components.

WP3 “Hardware Aware Crypto Building Block Design” builds suitable next-generation building blocks to obtain true hardware enabled cryptographic building blocks. Two approaches are pursued. While the first approach aims to explore to what degree cryptographic building blocks and countermeasures can accept imperfect random numbers before becoming insecure, the goal of the second approach is to design efficient crypto building blocks and countermeasures relying on higher-quality random number generators.

WP4 “Demonstration and Evaluation” showcases the work done in previous work packages through the design and realization of a hardware demonstrator, which will also be used both as a testing and an evaluation platform.

WP5 “Dissemination, Communication, Exploitation, Standardisation and Training” is in charge of the widespread diffusion of HECTOR concepts and results through publications and standardization actions and will furthermore cope with exploitation plans, business plans and intellectual property rights.

WP6 “Project-, Risk-, and Innovation-Management” shows dependencies to all other WPs as it coordinates and ensures that the tasks are in line with the project plan in order to reach the common goal of HECTOR.

Submitted Public Deliverables

- D5.1 *Internal and External IT Communication Infrastructure and Project Website*
- D5.2 *Data Management Plan (DMP)*
- D6.2 *Project Quality Plan*

Achieved Milestones

- MS1 *Successful project roll out*
- MS2 *Industrial requirements and Demonstrator*

Upcoming Public Deliverables

D2.1 *Report on Selected TRNG and PUF Principles*
D6.1 *Risk Assessment Plan*

Upcoming Milestones

- MS3 *PUF and TRNG principles selected*

PAST and ONGOING ACTIVITIES

After the successful project kick-off each partner has enthusiastically looked into their tasks within the particular WPs and started progress towards the objectives. We established a trustworthy working environment, which allowed an efficient collaboration within the first six project months and a timely submission of the first deliverables. **WP 1** reached a rough consensus about both what the evaluation platform should be and what the purpose of the demonstrator is. In total three use case scenarios were defined, requirements provided and a demonstrator proposed. In **WP2** a first portfolio on PUF types and post-processing methods has been established. Further, good progress understanding the influence of different noise sources within semiconductor devices vs. different TRNG principles has been made. The consortium will further focus on entropy estimations, metrics and PUF models, and further study on TRNG principles to be implemented on different embedded platforms. Moreover, an on-the-fly test for the DAC design will be developed. Within **WP3** an overview of specific cryptographic construction has been provided, forming the base for cryptographic primitives. Furthermore, two possible concurrent approaches for the evaluation of side-channel at design time have been introduced. Moreover, first proposals of a methodology determining security degradation were presented. Work will continue on developing key attack algorithms, investigating techniques for side-channel evaluations and defining degradations of random numbers relevant for countermeasures. Within **WP5** a project website and an information platform has been set up. Also, the design of a project logo, project leaflet, a poster and a roll-up has been settled and a system for data sharing has been proposed. Furthermore, results from **WP6** showed that the collaboration among partners is well functioning. The project management team performed work such as reporting to the EC, distributing the pre-financing, designing templates, and further handled day-to-day requests with partners and external bodies.

Start Date:	1 March 2015	***Consortium***:	9 partners (6 countries)
End Date:	28 February 2018	***Project Coordinator***:	Dr. Klaus-Michael Koch coordination@hector-project.eu
Duration:	36 months		
Project Reference:	644052	***Technical Leader***:	Bernard Kasser bernard.kasser@st.com
Project Costs & Funding:	€ 4.494.087,50		
		Scientific Leader:	Prof. Ingrid Verbauwhede ingrid.verbauwhede@esat.kuleuven.be

Project Website:
www.hector-project.eu

https://twitter.com/HECTOR_H2020