Newsletter

HECTOR

May 2016 - Issue 2

HECTOR

MISSION & MOTIVATION OF HECTOR

The mission of the HECTOR project is 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

Since the beginning of the project several conference calls and events dedicated to the project development took place. From 3rd to 4th of November 2015, the consortium met for the 1st technical & Advisory Board as well as General Assembly meeting in Paris. The focus of the meeting was the technical progress of each work package and the project in general. Special focus was devoted on the discussion about the manufacturing status of the evaluation boards. Moreover, the meeting brought lively discussions and a fruitful exchange with the experts of the Advisory Board. The 1st (interim) Review meeting hosted by the partner KU Leuven took place on 10th of December 2015. The progress of each WP was presented to the external reviewers and to the EC officer. The consortium received positive feedback and constructive recommendations for the upcoming project challenges. On the 9th and 10th of March 2016 the partners conducted a technical meeting, in Delft, Netherlands. Currently the consortium is preparing the next technical and GA meeting in Villach, Austria between 6th-7th of July 2016. Overall, the cooperation within the consortium is good and the project is well on track.

UPCOMING EVENTS

- **HOST 2016** – International Symposium on Hardware-Oriented Security and Trust, 5th – 7th of May 2016, Washington DC/USA
- **EuroCrypt 2016** - International Conference on the Theory and Applications of Cryptographic Techniques, 8th – 12th of May 2016, Vienna/Austria
- **Workshop and Training on Evaluation Boards,** 23th – 24th of May 2016, Leuven/Belgium
- **DAC 2016** – Design Automation Conference, 5th – 9th of June 2016, Austin, TX/USA
- **Technical and GA Meeting**, 6th – 7th of July 2016, Villach/Austria
- **CHES 2016** – Conference on Cryptographic Hardware and Embedded Systems, 17th – 19th of August 2016, Santa Barbara, CA/USA

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

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

Project Website:
www.hector-project.eu

https://twitter.com/HECTOR_H2020

Newsletter

HECTOR

May 2016 - Issue 2

HECTOR

TECHNICAL PROGRESS

WP1 ran from M01 to M06 and brought a common vision of everyone's expectations and requirements towards the security building blocks and technologies developed within the project. The WP1 ended with submission of deliverables D1.1 "Evaluation Platform and Industry-driven Requirements Specification" and D1.2 "Demonstrator-driven Requirements Specifications", which provided essential input for other technical WPs.

Within **WP2**, a first portfolio on PUF and RNG types was worked out including suitable post-processing methods. Evaluation criteria were defined and a prioritisation was done by the consortium. Deliverable D2.1 - Report on Selected TRNG and PUF Principles lists a first selection of different PUF and RNG types as well as a comparison of a set of evaluation criteria. It was the main outcome of WP2 in the first project months and will be an essential input for the work in WP3 and WP4.

WP3 kick-off meeting brought two possible concurrent approaches for evaluation of side-channel at design time. Partners provided an overview of specific cryptographic construction (Sponge construction), as well as first proposals of a methodology to determine security degradation. Furthermore, there has been development of a working setup for side channel analysis and perturbation attacks.

WP4 "Demonstration and Evaluation" will be kicked-off in August 2016.

STATUS OF HECTOR EVALUATION BOARDS

Discussions between the partners about the features of the evaluation board started from the outset of the project. Evaluation boards needed to be designed and manufactured as an optimized hardware target for implementation of TRNG s and PUFs. The schematic of the evaluation motherboard was completed within the first three months, as well as the printed circuit board design. Furthermore, a user manual for the motherboard was released by the partner Micronic. The partners will continue with the development and refinement of the evaluation boards and carry out a dedicated training session on the newly manufactured evaluation boards on 23rd May in Leuven, Belgium.

HECTOR PUBLICATIONS IN THE 1st PROJECT YEAR

- ***A Physical Approach for Stochastic Modeling of TERO-based TRNG*** in IACR Conference, 2015;
  P. Haddad, V. Fischer, F. Bernard, J. Nicolai
- ***Higher-Order Threshold Implementation of the AES S-box*** in CARDIS Conference, 2015;
  T. Cnudde, B. Bilgin, O. Reparaz, S. Nikova, V. Nikov
- ***Iterating Von Neumann's Post-Processing under Hardware Constraints*** in HOST Symposium, 2016;
  B. Yang, V. Rozic, W. Dehaene, I. Verbauwhede
- ***Using Reliability in Side-Channel Analysis of Binary-Field Multiplication*** in CT-RSA, 2016;
  P. Pessl, S. Mangard
- ***Analysis of the Kupyna-256 Hash Function*** in FSE, 2016;
  C. Dobraunig, M. Eichlseder, F. Mendel
- ***Square Attack on 7-Round Kiasu-BC*** in ACNS, 2016;
  C. Dobraunig, M. Eichlseder, F. Mendel
- ***Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript*** in DIMVA, 2016;
  D. Gruss, C. Maurice, S. Mangard
- ***Flush+Flush: A Fast and Stealthy Cache Attack*** in DIMVA, 2016;
  D. Gruss, C. Maurice, K. Wagner, S. Mangard

SUBMITTED DELIVERABLES & MILESTONES since the last newsletter

- D2.1 - Report on Selected TRNG and PUF Principles, R, PU, M12
- D6.1 - Risk Assessment Plan, R, PU, M12
- MS3 - PUF and TRNG principles selected, M12

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

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

Project Website:
www.hector-project.eu

https://twitter.com/HECTOR_H2020