Newsletter

HECTOR

January 2018 - Issue 4

HECTOR

We are now on the home straight... Almost.

The new year has just started and slowly but steadily the end of the HECTOR project is approaching. Officially the project should end in February 2018, but 3 of 6 work packages will be extended, while the budget remains the same. The reason for the extension is based on the fact that we promised at least one ASIC with at least one TRNG and one PUF principle design. As the arrival of the ASIC is only expected in March 2018, the focus of most of our evaluations would be on the FPGA implementations. In order to fulfil the technical exploitation and characterisation of the ASIC within the project lifetime the consortium requested the extension of the project by 5 months. This consentaneous internal decision was approved by the European Commission a few days ago. This will also allow the evaluation of the long term behaviour of the TRNG embedded tests implemented in FPGAs.

IN THIS ISSUE

Technical Meeting in Košice

In June 2017, Micronic hosted a technical face-to-face meeting in Kosice, Slovakia. As Micronic is located in Trebejov, which is only 20 km away from Kosice, the consortium was invited to visit the labs and the manufacturing facilities of the company. Micronic a.s. was founded in 1992 with the aim of providing electrical engineering services including development and manufacturing. In 1996, the team of Ladislav Cechlar began to work on its today's core business: development, production and sales of solutions for information security. It was a great experience being directly at the production line of our HECTOR evaluation boards.

Technical and Advisory Board Meeting in Saint Etienne

In September 2017, Université Jean Monnet Saint-Etienne hosted the HECTOR meeting at the Hubert Curien Laboratory in Saint-Étienne. From a technical point of view, we discussed the updates regarding the PUF and TRNG building blocks, focusing on their integration in the final HECTOR demonstrator. From a strategic point of view, we recapped the HECTOR outcomes against the formerly defined objectives, specifications and requirements. We also discussed the security evaluation performed by partner Brightsight. Beside our regular technical face-to-face assembly, four external advisors were invited in advance to join us for technical discussions: Werner Schindler from the German Federal Office for Information Security (BSI), David Lubicz from the French Department of Defense (DGA) and Patrick Haddad and Emmanuel Prouff from the French National Cybersecurity Agency (ANSSI). We presented the hot topics that we were repeatedly dealing with during the project lifetime. That included the lessons learned from HECTOR on TRNG design and the evaluation of their compliance with recommendations of BSI (AIS 31), with the last draft of NIST SP 800-90B and the requirements of the French DGA.

Start Date: 1st March 2015
End Date: 31st July 2018
Duration: 41 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

HECTOR

Newsletter

January 2018 - Issue 4

HECTOR

Technical Meeting in Delft

In December 2017, the HECTOR partner Brightsight hosted the technical meeting in Delft, The Netherlands. We had 3 intensive days focusing on the ASIC, the associated project extension, the security evaluation and the demonstrators rounded up with an official meeting of the General Assembly. To make the most of our time, we also worked closely together on Deliverable D4.2 ("Demonstrator Platforms") to ensure an accompanying report of sufficiently high quality that reflects our great collaborative work. The exploitation of the results beyond the project lifetime was another point on the agenda. Currently we are in the process of setting up a ***TRNG as a Service*** to let the community call up our research results across the network.

Recent Publications in HECTOR

- *Optimization of the PLL Configuration in a PLL-based TRNG Design*, Elie Noumon Allini, Oto Petura, Florent Bernard, Viktor Fischer. **Design, Automation and Test in Europe (DATE)**, 2018.
- *Towards Inter-Vendor Compatibility of True Random Number Generators for FPGAs*, Milos Grujic, Bohan Yang, Vladimir Rozic and Ingrid Verbauwhede. **Design, Automation and Test in Europe (DATE)**, 2018.
- *Spectral features of higher-order side-channel countermeasures*, Vittorio Zaccaria, Filippo Melzani, Guido Bertoni. **IEEE Transactions on Computers**, 2018.
- *Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices*, Raphael Spreitzer, Veelasha Moonsamy, Thomas Korak, Stefan Mangard. **IEEE Communications Surveys and Tutorials**, 2018.
- *KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks*, Michael Schwarz, Moritz Lipp, Daniel Gruss, Samuel Weiser, Clémentine Maurice, Raphael Spreitzer, Stefan Mangard. **The Network and Distributed System Security Symposium (NDSS)**, 2018.
- *Security Analysis of PUF-Based Key Generation and Entity Authentication*, Jeroen Delvaux. Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering, 2017.
- *Fast Leakage Assessment*, Oscar Reparaz, Benedikt Gierlichs and Ingrid Verbauwhede. **Conference on Cryptographic Hardware and Embedded Systems (CHES)**, 2017.
- *On-chip jitter measurement for true random number generators*, Bohan Yang, Vladimir Rozic, Milos Grujic, Nele Mentens and Ingrid Verbauwhede. **Asian Hardware Oriented Security and Trust Symposium (AsianHOST)**, 2017.
- *The Monte Carlo PUF*, Vladimir Rozic, Bohan Yang, Jo Vliegen, Nele Mentens and Ingrid Verbauwhede. **27th International Conference on Field-Programmable Logic and Applications (FPL)**, 2017.
- *Reconciling d + 1 Masking in Hardware and Software*, Hannes Gross, Stefan Mangard. **Conference on Cryptographic Hardware and Embedded Systems (CHES)**, 2017.
- *Efficient design of Oscillator based Physical Unclonable Functions on Flash FPGAs*, Ugo Mureddu, Oto Petura, Nathalie Bochard, Lilian Bossuet, Viktor Fischer. **Second International Verification and Security Workshop (IVSW 2017)**, 2017.

The HECTOR consortium is constantly publishing scientific articles. For all these publications open access is ensured via the open access repository Zenodo. We also created a dedicated community focusing on HECTOR related content: https://zenodo.org/communities/hector

Start Date: 1st March 2015
End Date: 31st July 2018
Duration: 41 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