ANNOUNCEMENT LETTER

HECTOR, a European cooperative research project, has officially started on 1st March 2015 with a set duration of 36 months. It has received funding from The European Union's HORIZON2020 Research and Innovation programme under grant agreement No. 644052.

EU Project HECTOR: Hardware Enabled Crypto And Randomness

A single flipped bit or a weak random number generator can cause secure systems to fail. The main objective of this research project is to **close the gap between the mathematical heaven of cryptographic algorithms and their efficient, secure and robust hardware implementations**.

It requires integrating secure cryptographic primitives such as:

- random number generators (RNGs), and
- physically uncloneable functions (PUFs), together with
- physical attack countermeasures.

Therefore we will **study, design and implement RNGs and PUFs** with demonstrable entropy guarantees and quality metrics, which includes:

- on-the-fly entropy testing and
- physical attacks evaluations.

This will **enable more secure systems and easier certification**. State-of-the-art cryptography and countermeasures can fail due to low-entropy random numbers. The unknown is 'how much' they will fail and how much entropy degradation can be tolerated (due to attacks or RNG designs mixing true and pseudo randomness).

Our objective is to **study the strength and gradual security degradation** when using lower entropy random numbers. This will enable more optimal and secure implementations. These objectives have to be combined with hardware efficiency and flexibility. This means addressing the extremely low-cost and low-power requirements of constrained embedded devices, low-latency of real-time memory encryption, or high throughput of future terabit networks.

Ultimately, we target security building blocks that are:

- flexible,
- hardware-friendly,
- efficient, and
- robust

against physical attacks, and which will be demonstrated on European relevant use cases.

The project leading to this application has received funding from the European Union's HORIZON 2020 Research and Innovation programme under grant agreement No. 644052.

TECHNIKON

HECTOR

We bring together experts from a carefully selected mix of 3 industry-, 3 academia and 3 evaluation lab partners with collective ambitions, potential and track records and with complementary expertise, dissemination and impact potential. Results will not only benefit the companies involved and their customers, but also the broader ICT through publications and inputs to standardization and certification bodies.

Project management of this 3-years project with 9 partners in 6 different countries is done by a professional company with an exceptional career track in EU project management.

This means the HECTOR consortium is well-positioned to achieve its objectives with the following 9 partners:

- Technikon Forschungs- und Planungsgesellschaft mbH, Austria
- Katholieke Universiteit Leuven, Belgium
- Université Jean Monnet Saint Etienne, France
- Thales Communications & Security SAS, France
- STMicroelectronics Rousset SAS, France
- STMicroelectronics SRL, Italy
- Micronic AS, Slovakia
- Technische Universität Graz, Austria
- Brightsight BV, Netherlands

For more information visit http://www.hector-project.eu (coming soon)

Contact information:

Project Coordinator

Dr. Klaus-Michael Koch
Technikon Forschungs-
und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
coordination@hector-project.eu

Scientific Lead

Professor Ingrid Verbauwhede
KU Leuven –
Department of Electrical Engineering
Kasteelpark Arenberg 10
3001 Leuven
Belgium
ingrid.verbauwhede@esat.kuleuven.be

Technical Lead

Bernard Kasser
STMicroelectronics
190 Avenue Celestin Coq-ZI
13106 Rousset Cedex
France

bernard.kasser@st.com

Disclaimer:

"The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose subject to any liability which is mandatory due to applicable law. The user uses the information at its sole risk and liability."

HECTOR:
Hardware enabled crypto and randomness

The project leading to this application has received funding from the European Union's HORIZON 2020 Research and Innovation programme under grant agreement No. 644052.