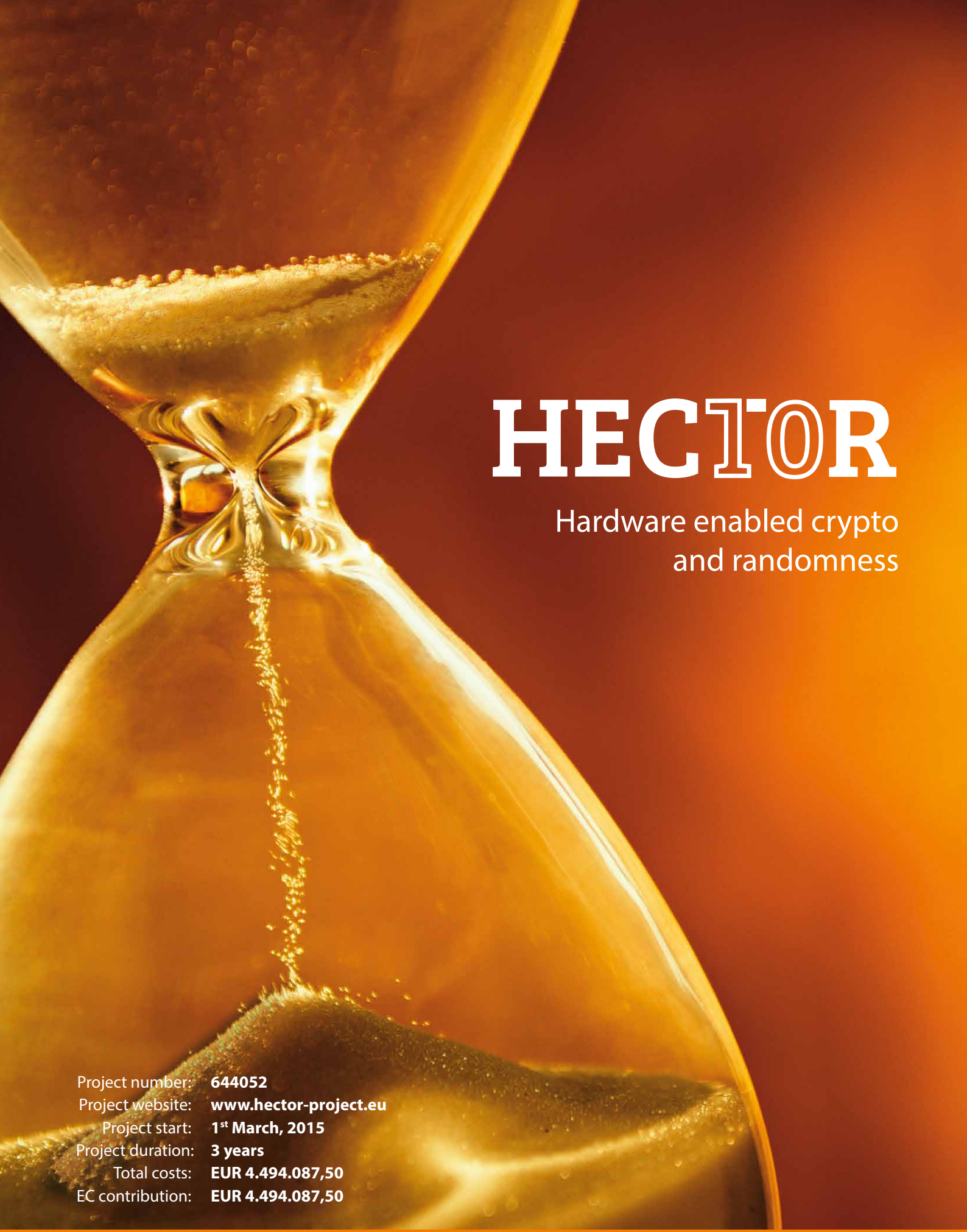
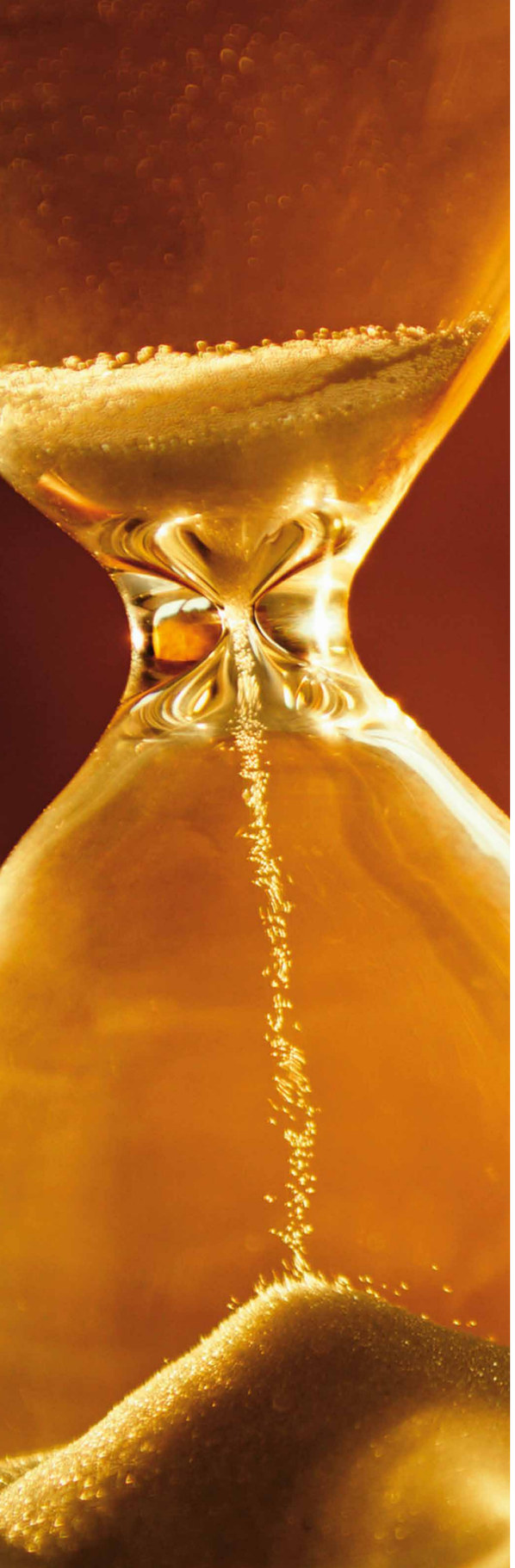


HECTOR

Hardware enabled crypto and randomness

Project number:	**644052**
Project website:	**www.hector-project.eu**
Project start:	**1st March, 2015**
Project duration:	**3 years**
Total costs:	**EUR 4.494.087,50**
EC contribution:	**EUR 4.494.087,50**

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



THE MISSION 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.

Motivation

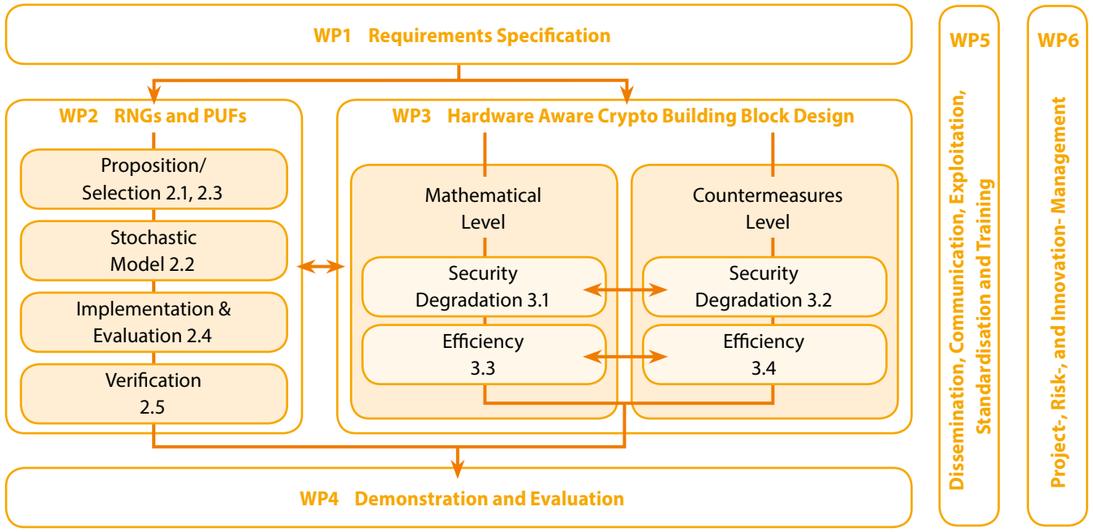
A single flipped bit or a weak random number generator can cause secure systems to fail. Therefore, the main motivation of this project is to bridge basic algorithmic approaches with hardware-level security implementations. It requires integrating secure cryptographic primitives such as random number 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.

Objectives

It is commonly accepted that the way cryptographic algorithms are implemented in hardware is at least as important as their mathematical robustness. Side-channel-attacks and hardware-attacks in general represent the most severe threats to modern cryptographic systems. Addressing the tension between mathematical security, implementation security and efficiency, as well as providing a holistic solution to the problem is at the core of the HECTOR project. Therefore, the main objective is to study the strength and gradual security degradation when using lower entropy random numbers, to enable more optimal and secure implementations. It has 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.

HECTOR structure and work packages

HECTOR



Technical Approach

The HECTOR project is planned to run 36 month. 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
WP1 intends to derive industry-driven requirements and specifications for the building blocks in WP2, WP3 and the demonstrator in WP4.

WP2 RNGs and PUFs
WP2 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. The derivation of a generic approach for the design and testing is an essential outcome of this WP to enable secure-by-design TRNGs and PUFs.

WP3 Hardware Aware Crypto Building Block Design
The third WP starts from existing algorithms and countermeasures in order to build novel designs with inherent protection against physical attacks. 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 as pursued in the second WP. Both approaches will be compared in terms of security and hardware efficiency. The final outcome is to build suitable next-generation building blocks to obtain true hardware enabled cryptographic building blocks.

WP4 Demonstration and Evaluation
The aim of WP4 is to showcase 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
WP5 wraps the project by focusing on dissemination, communication, exploitation, standardization and training. Hence, it 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
WP6 will interact with all other WPs in order to ensure a successful project lifetime with respect to risk- and innovation management. It 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.

Contact

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungs-
gesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55
E-Mail: coordination@hector-project.eu
Web: www.hector-project.eu

Scientific Lead
Prof. Ingrid Verbauwhede
KU Leuven - Department of Electrical Engineering
Kasteelpark Arenberg 10
3001 Leuven
Belgium
Tel.: +32 16 32 86 25
E-Mail: ingrid.verbauwhede@esat.kuleuven.be

Technical Lead
Bernard Kasser
STMicroelectronics
190 Avenue Celestin Coq - ZI
13106 Rousset Cedex
France
Tel.: +33 4 42 68 56 71
E-Mail: bernard.kasser@st.com

Consortium

The HECTOR consortium consists of a carefully selected mix of partners with collective ambitions, potential and track records and with complementary expertise, dissemination and impact potential in order to achieve its objectives. Altogether, there are 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 attack protection, as well as efficient hardware or embedded software implementations.

Project Partners

1 **Technikon Forschungs- und Planungsgesellschaft mbH**
Villach, Austria

2 **KU Leuven**
Leuven, Belgium

3 **Universite Jean Monnet Saint Etienne**
Saint-Etienne, France

4 **Thales Communications & Security SAS**
Paris, France

5 **STMicroelectronics Rousset SAS**
Rousset, France

6 **STMicroelectronics S.R.L.**
Agrate Brianza, Italy

7 **Micronic AS**
Trebejov, Slovakia

8 **Technische Universität Graz**
Graz, Austria

9 **Brightsight BV**
Delft, Netherlands