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

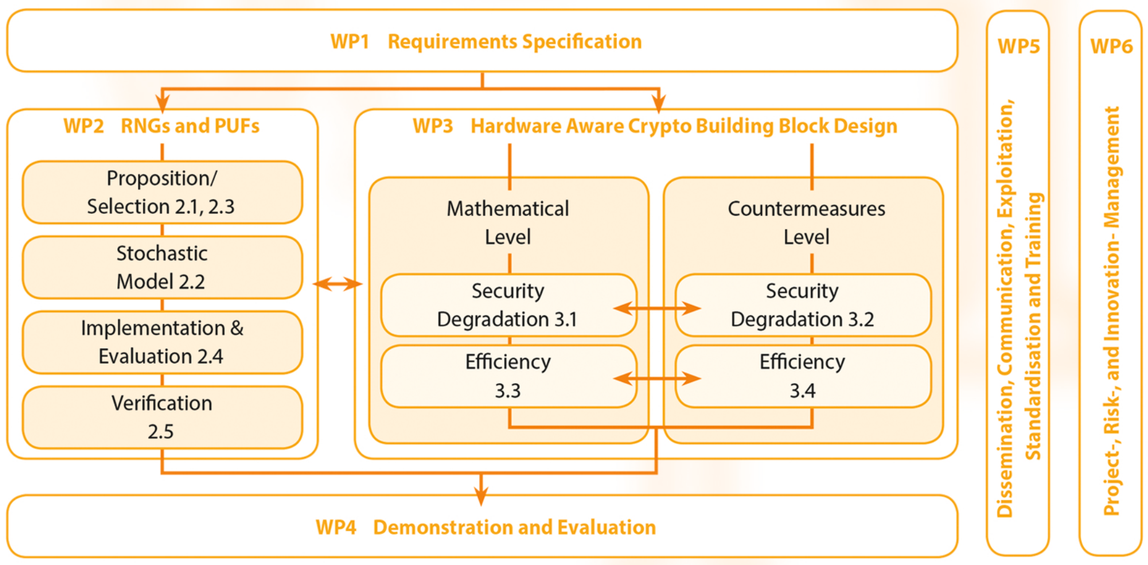
A single flipped bit or a weak random number generator can cause secure systems to fail. Therefore, the main motivation of this project is to bridge basic algorithmic approaches with hardware-level security implementations. It requires integrating secure cryptographic primitives such as random number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

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.



HECTOR

Project start: 1st March, 2015
Project duration: 3 years

Project Coordinator
Dr. Klaus-Michael Koch
Technikon Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
Tel.: +43 4242 233 55

Scientific Lead
Prof. Ingrid Verbauwhede
KU Leuven - Departement of
Electrical Engineering
Kasteelpark Arenberg 10
3001 Leuven, Belgium
Tel.: +32 16 32 86 25

Technical Lead
Bernard Kasser
STMicroelectronics

190 Avenue Celestin Coq - Zl
13106 Rousset Cedex, France
Tel.: +33 4 42 68 56 71

www.hector-project.eu
coordination@hector-project.eu

This project has received funding from the European Union‘s Horion 2020 research and Innovation programme under grant agreement No. 644052.