	FPGA-based implementation of Cryptographic Algorithms for the Advanced Open-source Security Platform SE*cube*™
Parole chiave	SECURITY, HARDWARE DESIGN, FPGA-BASED DESIGN, CRYPTOGRAPHY, CRYPTOGRAPHIC ALGORITHMS, EMBEDDED SYSTEMS, DIGITAL SYSTEM DESIGN, SYSTEM LEVEL DESIGN & TEST, OPEN-SOURCE
Riferimenti	Paolo PRINETTO
Riferimenti esterni	Pascal TROTTA (PhD student), Giuseppe AIRO´ FARULLA (PhD Student), Giorgio DI NATALE (LIRMM, Montpellier, France).
Gruppi di ricerca	TESTGROUP - TESTGROUP
Tipo tesi	EXPERIMENTAL
Descrizione	***Motivations***: Nowadays, many services and applications need to be secured in order to guarantee the users' privacy as well as the commercial and legal issues related to security threats and to safeguard the business stakeholders. While several standards, protocols and algorithms exist for handling the basic primitives for security (i.e., confidentiality, authentication, privacy), their implementation in real objects may require very high expertise and efforts. The development of the Advanced Open-source Security Platform SE*cube*™ (Secure Environment Cube) tries to fill this gap providing heterogeneous security-oriented hardware, coupled with an open-source modular software architecture In the Platform, all the functional blocks are isolated and well documented in order to deliver to developers an easy-way to build, understand, modify, and rewrite the whole system if wanted. The SE*cube*™ hardware consists of a single System-on-Chip (SoC) composed of three main blocks: (i) a low-power ARM Cortex-M4 processor, (ii) a flexible and fast Field-Programmable-Gate-Array (FPGA), and (iii) an EAL5+ certified embedded SmartCard. All these features make the SE*cube*™ platform perfectly suitable for a wide range of applications where security is a major concern, including, among the others, Telecommunications, Internet of Things, and Home Automation. In order to provide additional custom security features, several cryptographic algorithms, other than the ones already offered by the embedded certified SmartCard, can be implemented in the SE*cube*™ platform FPGA module. The flexibility offered by the FPGA can be effectively exploited to design very fast custom hardware accelerators implementing the chosen algorithms (e.g., DES, AES, …). ***Goal of the thesis***: • Hardware implementation (VHDL/Verilog) of selected cryptographic algorithms targeting the SE*cube*™ platform FPGA module, under timing and power constraints. • Implementation of software drivers to allow the SE*cube*™ processor to access the hardware modules implemented in the FPGA and send/receive

their input/output data.

Learning outcomes:

The student will improve its VHDL/Verilog coding skills and digital systems design knowledge.
Moreover, she/he will understand the entire design flow of hardware modules, starting from requirements definition to logic simulation and synthesis with state-of-the-art EDA tools.
Finally, she/he will be able to test and debug designed modules on actual hardware (i.e., SE*cube*™ and/or other commercial FPGA development boards).

External/Industrial cooperations:

The thesis will be carried out in collaboration with:

- *Blu5* View Pte. Ltd. (Singapore)
- *CINI CyberSecurity National Lab,* Nodo di Torino (Torino, Italy)
- *Lero*, the Irish Software Research Centre (Limerick, Ireland)
- *LIRMM* (Montpellier, France).

Conoscenze richieste	Programming Languages: VHDL or Verilog, C / C++ Digital System design methodologies, Computer Architecture, FPGA
Note	Number of required Students: 1 or 2
Scadenza validita proposta	31/12/2016

PROPONI LA TUA CANDIDATURA