CCE_7

Title of the doctoral program

Computer and control engineering

Title of the research activity

Hardware Security for Future Technologies - Security Primitives

Short description of the research activity

In today CMOS the short-comings caused by technology scaling are becoming more relevant than the benefits. To overcome these shortcomings, novel technologies are being currently under research, to identify the best candidate to replace today charge based devices. Amongst these, the most promising so far, are the memristive elements and spin-based devices. In both traditional and emerging technology electronics, the data security is essential to assure a dependable system. The research activity of this project will be centered on hardware security aspects for new generation electronic devices, with special emphasis on security primitives. During the duration of the thesis, the candidate will study and develop solutions for Physically Unclonable Functions (PUFs), Random Number Generators, combinational logic for security, fast and secure erasing, etc. All these solutions will be centered on the special characteristics of the future, non-charge based, technologies.

Scientific responsible (name, surname, role, email)

Paolo Prinetto, Full Professor, paolo.prinetto@polito.it

Number of vacancies for XXXI cycle (3 years program)

1

Specific requirements (experiences, skills)

Basic knowledge of cryptography, Basic knowledge of digital circuit design.

Website of the research group (if any)

www.testgroup.polito.it