POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 40th cycle

Research Area n. 1 - Computer Science and Engineering

THEMATIC Research Field: HARDWARE SUPPORT FOR SECURE RISC-V MICROPROCESSORS

Monthly net income of PhDscholarship (max 36 months)
€ 1400.0 In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity	
Motivation and objectives of the research in this field	Computing platforms for modern embedded systems, e.g., automotive systems or next generation satellites, are required to be flexible, high-performance and low-cost. To achieve these requirements, integrated circuits are produced following a globally distributed design flow: the System-on-Chip (SoC) will integrate modules designed in-house with other modules coming from third party entities, either in the form of Third-Party IP cores (3PIPs) or in the form of Commercial Off-the-Shelf (COTS) components. Moreover, the final fabrication of the silicon device will rely on outsourced foundries. While ensuring high-performance and reduced cost, such globalized design process exposes the obtained system to several security threats both at design time and at runtime. In particular, purchased IP cores may contain unwanted functionalities or the final produced integrated circuit may be maliciously modified. Such stealthy unwanted functionalities are known as Hardware Trojan Horses (HTHs).The goal of the PhD is to the system *Intelligent Security Checkers (ISCs)* meant for monitoring the activity carried out by the microprocessor and to detect at runtime the activation of HTHs and Transient Execution Attacks, e.g., Spectre and Meltdown. As a beneficial additional side-effect, such ISCs would also allow to detect anomalous behaviors due to random faults (e.g. Soft Errors in memories, SEUs in

	registers) instead of malicious attacks. Of course, it is mandatory for the introduced security checker not to interfere with the nominal functioning of the system, i.e., not to introduce working frequency slow-down, and to bring the smallest possible silicon area and power consumption overhead.
Methods and techniques that will be developed and used to carry out the research	The PhD student will exploit techniques based either on probabilistic data structures or on machine-learning to develop the Intelligent Security Checkers required for attack detection.Moreover, architectural and microarchitectural modification of the considered microprocessors may be required in order to make attacks unfeasible of less likely.Finally, both software-based simulation and HW prototyping will be required to evaluate the effectiveness of the proposed security solution as well as their impact on the power consumption of the system, on silicon area occupation of the chips and on the global working frequency, i.e., performance drop.
Educational objectives	The PhD student will acquire deep knowledge regarding the architectures of modern microprocessors and about how to modify them in order to increase security. Moreover, the PhD student will be required to understand the most significant security threats for integrated circuits, e.g., HW Trojan Horses and Transient Execution Attacks.
Job opportunities	The PhD student will acquire knowledge and competencies that will make him/her a strong digital designer as well as HW security engineer both at the circuit- and at the system-level for companies working in the field of integrated circuits (with particular emphasis on microprocessors) such as Intel, NVIDIA, Microchip, Frontgrade, SiFive as well as for companies and institutions working in the field of system engineering such as Thales Alenia Space, NASA and ESA.
Composition of the research group	0 Full Professors 1 Associated Professors 0 Assistant Professors 0 PhD Students
Name of the research directors	Prof. Luca Maria Cassano

Contacts
luca.cassano@polimi.it

Additional support - Financial aid per PhD student per year (gross amount)	
Housing - Foreign Students	--
Housing - Out-of-town residents (more than 80Km out of Milano)	--

Scholarship Increase for a period abroad	
Amount monthly	700.0 €
By number of months	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information

EDUCATIONAL ACTIVITIES: purchase of study books and material and funding for participation in courses, summer schools external to Politecnico di Milano: financial aid up to 5707,20 Euro.

TEACHING ACTIVITIES: the PhD student could support the teaching activity of the supervisor both in the bachelor course of Fondamenti di Informatica and in the master course of Design of Hardware Accelerators.

Computer and desk availability: the PhD student will require a desk and possibly a workstation PC more powerful than his/her personal laptop. Possibly additional equipment, e.g., FPGA-based development boards, software licenses, will be purchased: financial aid according to the availability of the Advisor'sfunds.

Premialities will be recognized to the PhD candidate. Up to 3000 euro (gross amount) after the completion of the 1st year; up to 3000 euro (gross amount) after the completion of the 2nd year; Up to 3000 euro (gross amount) after the completion of the 3rd year. The premialities will be assigned provided that she/he demonstrates a significant contribution to the growth of scientific excellence, the industrial valorization of research, the networking and communication activities of the Department.