POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 39th cycle

Research Area n. 1 - Computer Science and Engineering

PNRR 117 Research Field: SIDE-CHANNEL RESISTANT CRYPTOSYSTEMS FOR HIGH-BANDWIDTH MEMORIES

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	Modern Solid-State Drives (SSD) embedded in Personal Computer (PC), datacenter and automotive application environments, offer a set of security properties for the computing system to which they are connected. Among such properties there are the authentication of the memory module, and the confidentiality and integrity of user data. To achieve the former, a per-device unique secret needs to be either stored securely or derived from the inherent properties of each device. As for the latter, in order to ensure the confidentiality and integrity of user data, cryptographic systems are usually employed, generically called “self-encryption technologies”, that enable the drive to autonomously encrypt the received data before storing it into a non-volatile SSD, e.g., NAND. Such cryptosystems thus guarantee the aforementioned properties, without decreasing the performance figures of the device itself, and providing protection against physical threats, where an attacker might attempt at extracting data from the device without the consent of the owner. However, secret storage has proven to be vulnerable against physical readout attacks, and the cryptosystems employed in both authentication and data protection schemes might be vulnerable against Side-Channel Attacks. The objective of this research is then to assess

	the susceptibility of real-world devices against Side-Channel Attack methodologies, including non-profiled and profiled attacks. Furthermore, the research should design cryptographic systems that are able to withstand the bandwidth and latency requirements of storage devices, e.g., SSD, and that, at the same time, can provide mitigations against Side-Channel Attacks. Finally, a suitable solution to the guarantee of the device identity should be studied and developed.
Methods and techniques that will be developed and used to carry out the research	The research activity requires the development of innovative methods that enable the application of Side-Channel Analysis techniques against high-frequency HW pipelined realizations of data-storage-oriented cryptographic mode-of-operations. These methods include techniques for the detection of cryptographic operations in a continuous data stream, and methods for exploiting the correlation in pipelined implementations. Regarding the development of novel cryptosystems, a set of techniques should be derived to realize side-channel resistant cryptosystems in an area-constrained environment, with demanding bandwidth-latency requirements. The design of identity-storage mechanisms will require the development of tools to protect the secrets against physical inspection, including the design and use of Physical Unclonable Functions (PUF). As many PUF solutions now employ a Static Random Access Memory (SRAM) block as a source of device-unique entropy, the security evaluation of PUFs of that type will also require the development and experimentation of attacks that exploit the analysis of laser-induced side channels to extract contents from SRAM blocks.
Educational objectives	The PhD candidate will acquire an extensive knowledge of the security threats to the hardware devices that include cryptography-based security functions. In particular, the candidate will acquire knowledge in the practical application of Side-Channel Analysis strategies against complex targets, and will develop the design skills required for designing a side-channel resistant cryptosystem that is fit for a high-performance computing

	environment. The candidate will also become confident with the problems and the potential solutions of the secret storage and derivation in high-performance storage and memory devices.
Job opportunities	This PhD program is sponsored by a global silicon manufacturer company, and the research activity will be conducted also in the company laboratories. This will result in a broad exposure of the skills of the candidate towards the company management, which may lead to the hiring of the PhD candidate at the end of the program. In any case, the skills and experience acquired by the candidate during the research activity are highly requested in the industrial talent market. Therefore this PhD program provides good opportunities for employment in the job markets, both national and international.
Composition of the research group	0 Full Professors 4 Associated Professors 2 Assistant Professors 4 PhD Students
Name of the research directors	prof. Luca Oddone Breveglieri

Contacts
luca.breveglieri@polimi.it. +39 02 2399 3653, www.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

National Operational Program for Research and Innovation	
Company where the candidate will attend the stage (name and brief description)	MICRON SEMICONDUCTOR ITALIA SRL
By number of months at the company	6
Institution or company where the candidate will spend the period abroad	Télécom Paris

candidate will spend the period abroad (name and brief description)	
By number of months abroad	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information
EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student. TEACHING ASSISTANTSHIP: availability of funding in recognition of supporting teaching activities by the PhD student There are various forms of financial aid for activities of support to the teaching practice. The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations. COMPUTER AVAILABILITY: individual use. DESK AVAILABILITY: individual use.