POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 38th cycle

Research Area n. 1 - Computer Science and Engineering

PNRR_352 Research Field: SYNTHETIC MODELS FOR SIDE CHANNEL ATTACK ANALYSIS AND COUNTERMEASURE DEVELOPMENT

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	Side channel attacks are one of the prime threats to the security of modern digital computing systems. Indeed, the ubiquity of the computing devices has led to their deployment in unsupervised environments where attacker may easily gain physical access to them. The large variety of computing platforms requires currently a tailored approach to understand the nature of the information leakage via side-channel, and to mitigate such vulnerabilities. This increasing engineering effort imposes a significant cost on the design of secure systems This research aims at providing synthetic models of side channel information leakage, which will in turn allow to: i) quantify how effective are current data-driven attacks are in extracting information, ii) design countermeasures which can be proven to be thwarting them.
Methods and techniques that will be developed and used to carry out the research	The research will develop power consumption and EM radiation models (both architectural and micro-architectural) linking the data processed by the digital computers to their side channel behavior. Such models will be turned into practically usable artifacts implementing device simulators and attack procedures. From a

	technology standpoint, the outcome of the research is expected to be a set of tools providing the capability to a designer to obtain synthetic estimations of the side channel leakage, and validating the effectiveness of the countermeasures against such an information leakage.
Educational objectives	The candidate will acquire the skills necessary to conduct advanced research at universities, public bodies, or private organizations for the purpose of advancing scientific and technological progress in the context of applied cryptography, computer architectures and computer security. The candidate will perform the following tasks: prepare a doctoral thesis in Computer Security and Cryptography; publish research papers and give talks at the top international venues; provide guidance to M.Sc. students and work as teaching assistant for classes, on a voluntary basis; organize science outreach activities.
Job opportunities	A cryptography engineer is an information technology professional who specializes in securing data and communications designing systems that exhibits provably security features to the end of preventing non authorized users from hacking data. Cryptography engineers work for a variety of employers. Some are in law enforcement, while most work in the private sector and help their clients or employers secure their data from all security threats.
Composition of the research group	0 Full Professors 3 Associated Professors 0 Assistant Professors 2 PhD Students
Name of the research directors	Gerardo Pelosi, Alessandro Barenghi

Contacts
gerardo.pelosi@polimi.it, 0223993476, https://pelosi.faculty.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)	Nome impresa: STMicroelectronics (Agrate, Italy) S.r.l. Settore attività: Elettronica e semiconduttori. https://www.st.com/content/st_com/en.html
By number of months at the company	6
Institution or company where the candidate will spend the period abroad (name and brief description)	Nome azienda: STMicroelectronics (Rousset, France) SAS Settore attività: Elettronica e semiconduttori. https://www.st.com/content/st_com/en.html
By number of months abroad	6

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

Attinenza alla tematiche, alle missioni/componenti prescelte del bando PNRR v. D.M. 352, art.6

Il dottorato di ricerca mira a formare il candidato nell'ambito della sicurezza informatica e della crittografia applicata. Entrambi gli ambiti sono di forte ed attuale interesse, e le occasioni di formazione sopratutto in ambito di crittografia applicata per lo sviluppo di piattaforme di calcolo sicure contro attacchi side channel sono relativamente poche al momento in Italia. La cybersecurity è stata identificata come una delle key enabling technologies della missione 4, componenete 2 del PNRR, e la professionalità di un cryptography engineer concorre a pieno all'allargamento delle competenze e conoscenze italiane in tale ambito.

Impresa, presso cui si svolgerà l'attività esterna

STMicroelectronics S.r.l.
Nello specifico i tre macro-settori principali si classificano in
1)Microcontrollers and Digital ICs - composto da microcontrollers di uso generale e di sicurezza;
2)Analog and MEMS - circuiti integrati analogici a bassa potenza high-end; dispositivi smart power per mercati industriali; soluzioni di connettività a bassa potenza (sia con cavo che wireless) per IoT.
3)Automotive and discrete components - circuiti integrati dedicati per il settore automotive (sia digitali che analogici), e i prodotti separati e i transistor di potenza.
Descrizione sintetica dell'attività in STM Agrate: analisi delle vulnerabilità micro-architetturali di microprocessori RISC

Ente, università, azienda, centro di ricerca presso cui si svolgerà il periodo di studio e

ricerca all'estero.

STMicroelectronics (Rousset, France) SAS
Nello specifico i tre macro-settori principali si classificano in
1)Microcontrollers and Digital ICs - composto da microcontrollers di uso generale e di sicurezza;
2)Analog and MEMS - circuiti integrati analogici a bassa potenza high-end; dispositivi smart power per mercati industriali; soluzioni di connettività a bassa potenza (sia con cavo che wireless) per IoT.
3)Automotive and discrete components - circuiti integrati dedicati per il settore automotive (sia digitali che analogici), e i prodotti separati e i transistor di potenza.
Descrizione sintetica dell'attività in STM Rousset, France: attività sperimentale relativa alla validazione dei modelli di perdita di informazione e efficacia delle contromisure sviluppate durante l'attività di ricerca principale, facendo uso delle attrezzature di laboratorio degli altri centri di ricerca consortili del Centre Microélectronique de Provence di cui STMicroelectronics Rousset fa parte.

**All information regarding educational activities, personal funding, regulations and obligations of Ph.D. candidates are available on the
web site https://dottoratoit.deib.polimi.it/**