TRUDEVICE Short Term Scientific Missions Application

ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

Involved Institutions

Home Institution: Luis Andrés Cardona, Carles Ferrer; Universitat Autònoma de Barcelona, Barcelona, Spain

Host Institution: Luca Sterpone, Ernesto Sanchez; Politecnico di Torino, Turin, Italy

Visit Details

Visiting Researcher: Luis Andrés Cardona

Visiting Period: 01/10/2014 – 07/01/2015

Mission Statement

My research interests are in the area of fault tolerant embedded systems using reconfigurable devices for critical and cryptographic applications.

Reconfigurable devices, specifically SRAM-based FPGAs, are of great interest in the design of flexible embedded system. By using partial reconfiguration, certain hardware components can be dynamically adapted to the requirements of the application. But as countermeasure this flexibility makes them more susceptible to faults and external attacks. Single Event Upsets can alter the physical implementation of the hardware by modifying the configuration memory. If the memory content that define the behaviour and connectivity of the internal components of the device or the application data are attacked, defective functioning of the system can be produced.

To overcome the mentioned limitations, alternative design methods should be investigated. In this context, the mission has as main objective to explore new mitigation techniques applied to SRAM-based FPGAs combined with partial reconfiguration to obtain self-repair systems. In addition, fault injection campaigns will be carried out to analyse the architectural designs. These goals fit into the activities of the WG4: Reconfigurable devices for secure functions, and WG5: Validation, Evaluation, and Fault Injection.

The expertise of the Host Institution in the described topics makes it an excellent destination to promote collaboration, learn about different methods and take some measurements that allow us to investigate and improve the explored techniques.

The general activities of the visit are summarized in Table I.

Budget Request

Travel: 300 €
Accommodation: 3 * 400 €/month = 1200 €
Meals + Transport: 99 * 20 €/day = 1980 €
Total: **3480** €

Table I: Planned activities for the STSM

Id.	*Activity*	*T4 14*			
		oct	*nov*	*dic*	*ene*
1	Study and implementation of fault detection and correction techniques in SRAM-based FPGAs required to design self-repair systems				
2	Evaluation of the implemented techniques in terms of its influence in performance, area and resistance against external attacks				
3	Study of analytical models such as availability, fault models, fault coverage, to investigate architectural alternatives of the systems				
4	Test of the implemented architectures using simulation tools or fault injection. One possible alternative is to emulate faults by changing the configuration memory bits				
5	Consolidation of the results obtained from the previous steps and preparation of reports and papers				