Doctoral thesis summary

UPC
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola de Doctorat

DNI/NIE/passport	CJ 174139			
Full name	NEAGU MĂDĂLIN-IOAN			
Title of the thesis	SELF-HEALING AND SECURE LOW-POWER MEMORY SYSTEMS			
Structural unit	DEPARTMENT OF ELECTRONIC ENGINEERING			
Programme	ELECTRONIC ENGINEERING			
UNESCO codes	330700			

(Minimum 1 and maximum 4; see the codes at https://doctorat.upc.edu/academic-management/formsfolder/thesis-registration-and-deposit/unesco-codes)

Thesis summary of a maximum of 4,000 characters (if you exceed this number it will automatically cut you off).

The main objective of this thesis is to bring new contributions to the self-healing and secure systems domain. In particular, to develop a self-healing technique for memory systems and to increase security of memory systems, techniques which favor low-power consumption. In order to achieve the main objective, three major research objectives were proposed: design of an error detection and correction scheme for errors that occur in memory systems and integrate them in a memory system, design techniques to increase the security and data privacy of memory systems against different types of attacks and to combine the previous two into a single solution, in order to achieve a self-healing and secure low-power memory system. The low-power aspect of the proposed solutions and techniques is evaluated during design stage and afterwards through simulation. Also, the architectures are evaluated from several other points of view, such as error detecting and correcting performance, area and delay overhead, and security efficiency.

The first chapter contains a short introduction of the domain and subject of the thesis, current state of the art in this domain, proposed objectives and thesis organization.

The second chapter contains a unidirectional error detecting, correcting and localization scheme, which is used for the self-healing technique. The chapter begins with an introduction and motivation about error detecting and correcting codes and their usage in memory systems and continues with a theoretical background. The chapter continues with the design of the proposed codes, which are explained in detail and illustrated through several figures. Then, they are analyzed from the following points of view: coding scheme, error localization, error correction and error escapes. For the latter three, metrics are defined, in order to evaluate the codes. Afterwards, the implementation of the proposed codes is exposed in several figures. Also, the usage of the codes is explained, as well as DRAM repair strategies. In the end of this chapter, the efficiency of the proposed codes is evaluated and exemplified. The evaluation process contains other metrics: speed and delay, area overhead, power consumption and code redundancy.

Chapter 3 contains a proposed scheme to increase security in memory systems against cold-boot attacks. The technique uses data scrambling, hence the chapter begins with a short theoretical background and a review of data scrambling methods. It continues with the proposed solution, which is based on using unique scrambling vectors in an interleaved way, and theoretical performance and efficiency. The chapter ends with evaluation and experimental results for the proposed methodology. Evaluations of area overhead, power consumption and access time are performed in the CACTI simulation tool and on a FPGA development board.

Chapter 4 approaches specific types of threats that can prevail in memory systems: simple and differential power or electromagnetic analysis attacks (SPEMA and DPEMA). The chapter begins with short introduction and motivation sections, and continues with a theoretical background about possible threats. In the following section, SPEMA and DPEMA are explained and discussed in detail. Afterwards, the proposed solutions for mitigating SPEMA and DPEMA are exhibited, and ends with evaluation and experimental results. An information leakage function is defined and used in evaluating the security efficiency of the solutions. The implementation costs are assessed with the use of the CACTI simulation tool, with respect to area and delay overhead, and power consumption.

The final chapter, 5, contains the conclusions of the work, scientific contributions and future research directions.

Place	BARCELONA	Date	22-05-2017

Signature

Neagu