Call for applications - PhD candidate

Exploration of security threats in In-Memory Computing Paradigms

Location: TIMA Laboratory (AMfoRS team), Grenoble, France
Funding: 3-year PhD grant, ~1770€/month (brut) – EEATS Doctoral School Scholarship
Starting date: September 2019
Key-words: hardware security, In Memory computing

Context

Security is critical today for information and communication technologies. It is the basis for obtaining confidentiality, authentication, and integrity of data. Improving the attack resilience of secure devices is a major challenge today due, in part, to the accelerated race among the developers and the attackers, and also to the heterogeneity of new systems and their ever-increasing numbers. The vulnerabilities of electronic devices that implement cryptography functions have been well studied in the last decade for *von Neumann* computing architectures, designed with CMOS technology. However, there is little evidence that these studies hold true for novel computing paradigms with new technologies.

In-memory computing paradigm is an emerging concept based on the tight integration of traditionally separated memory elements and combinational circuitry. It allows the minimization of the time and the energy needed to move data across the processor. The most promising solutions for in-memory computing architectures are based on the use of emerging technologies (Spin Transfer Torque RAM and Redox RAM) that are able to act as both storage and information processing unit. Despite the promising nature of the in-memory computing-based architectures many issues related to the devices themselves and to their double usage (storage and computing unit) need still to be solved. In particular, a correct evaluation of security threats targeting systems based on in-memory computing is still missing.

The **innovative aspects** of this PhD are related to the security aspects to be considered for a In Memory computing implementation. Indeed, the tight coupled memory-computing elements vulnerabilities have to be analyzed in hybrid NV-CMOS technologies. This research direction is very ambitious and can lead to consequent research direction.

The **main objectives** of this thesis are twofold:

> Establish a taxonomy of attacks – identification and classification of possible attacks that can lead to exploitable errors (i.e., that can jeopardize the security of the application) or leak of information in an in-memory crypto-processor architecture.
>
> Provide justified comparison between in-memory mapping techniques – Several methods exist in literature allowing mapping of any logic function on in-memory computing structures. Our objective is to map a crypto-processor algorithm in the corresponding in-memory architecture by using different mapping approaches, thus obtaining several in-memory crypto-processor versions with different characteristics. We will compare the resilience of these circuits to the proposed attacks.

To fulfill the proposed objective, we have identified the following activities:

> The first activity will focus on the definition of fault models of at bit-cell and circuit level, and on the information leakage analysis in order to address both fault and side-channel attacks. After a literature review, we will build device models to be simulated at physical level (TCAD simulators). The extracted

information will be used to build higher-level abstractions of faults that will be simulated at electrical level (spice/veriloga simulators) on processing-in memory matrix.

The second and third activities will be dedicated to the mapping of logic functions on In-Memory matrix and architectures. We will then synthesize the basic building block of encryption algorithms (like substitution boxes, XORes, multiplexers, Feistel schemes, coders and decoders) using known tools (e.g., Xbargen) on memristive-based In-Memory architectures.

In n the last activity, we will study the correlation between in-memory computation power and switching profiles to understand if side-channel analysis will allow the leakage of information, and we will analyze internal perturbations (timing, power supply, temperature) to understand the circuit's intrinsic resistance in front of perturbation attacks. All these analyses will be performed by electrical-level simulations, thanks to the model developed in the first activity.

Profile: Master degree or equivalent in the area of either Electronic Engineering or Computer Science.

Expected skills

Technical: Analog/Digital integrated electronics (design, HDL modeling languages, CAD tools), C/C++ and scripting. Knowledge about front end/back end, assembly language, machine learning algorithms, data science, etc.
Personal: Determination, perseverance, trustworthiness, autonomy, adaptability, initiative, good communication skills
Languages: English: at least B2 equivalent, excellent reading and writing level, good speaking level. Fluency in French is a plus but it is not mandatory.

About TIMA
TIMA Laboratory is a public joint research laboratory located in Grenoble, France, and held jointly by Institut Polytechnique de Grenoble (Grenoble INP), University Grenoble-Alpes and French National Research Council (CNRS). TIMA is a multinational team of over 100 people, with members and interns from all over the world. The research topics of TIMA cover the specification, design, verification, test, CAD tools and design methods for integrated systems, from analog and digital components on one end of the spectrum, to multiprocessor Systems-on-Chip together with their basic operating system on the other end.
This call is from the AMfoRS team, and targets people motivated by hardware security and test. More information about the team is available at http://tima.imag.fr/tima/en/AMfoRS/AMfoRSoverview.html

Advisors
Main advisors: Lorena Anghel, Professor, Grenoble INP, Giorgio di Natale, Director of Research in CNRS and Ioana Vatajelu, CNRS Researcher.
The work will be carried out in strong cooperation with the other members of the team with large experience background in security and design;

To apply, send a mail to lorena.anghel@univ-grenoble-alpes.fr, **giorgio.di-natale@univ-grenoble-alpes.fr or** ioana.vatajelu@univ-grenoble-alpes.fr with the following attachments (in English or French):
- Detailed curriculum vitae
- Application letter with clear motivations
- Academic transcripts for the last two years of study
- 2 or 3 recommendations (letters or reference persons with e-mail addresses)