PhD Thesis Proposal at LIRMM (University of Montpellier, France)

Topic : Exploration of In-Memory Computing architectures for secure systems

Context

The important growth of Internet of Things (IoT) is leading to the so-called Big Data, where a huge amount of data require to be stored, encrypted and processed in a fast, reliable and secure way.
Today's architectural solutions require very high amount of power consumption as well as execution time. Actually, most of the time and energy is spent in the exchange of the information from the memory to the processing units and back. This waste of time and energy is exacerbated by the fact that, in order to increase the overall performance of the system, several layers of caches are used in computing systems.

In order to deal with the forthcoming data explosion, the research community is exploring innovative in-memory computing architectures (exploiting emerging device technologies) to overcome the above limitations for future energy efficient and high performance systems.
Recent advances on non-volatile memories implemented with emerging technologies have enabled the design of compact, high-speed, energy-efficient in-memory computing elements. Nevertheless, security implications of such a new technology are not yet covered.

Problem Statement

We want to study and exploit in-memory-computing for data encryption and security, and possibly open the way to the future standard for the security of information in Big Data and IoT applications.

Indeed, such a new technology might enable the implementation of novel encryption methods. More in particular, homomorphic cryptography (i.e., a type of encryption that allows performing operations on encrypted operands) is nowadays too expensive in terms of computation time and power consumption with classical computing architectures. However, It is therefore possible to take advantage of the in-memory computing paradigm to overcome current limitations.

Objective

The goal of this thesis is to explore the characteristics of new technologies and architectures for in-memory computing in applications requiring security. The PhD thesis will focus on:

- Novel technologies for in-memory computing
- The in-memory computing paradigm
- The security provided by new technologies, especially with respect to their resistance to hardware attacks such as side-channel attacks
- Application of in-memory computing paradigm to homomorphic encryption

Requirements:

- Hold a university degree equivalent to a bachelor's degree or higher.
- Have a good command of English.
- Good skills in electronics and electrical engineering
- Good skills in C programming, VHDL, Computer architectures.
- Basic skills in Cryptography

Contacts:

giorgio.dinatale@lirmm.fr +33 4 67 41 85 01
bruno.rouzeyre@lirmm.fr +33 4 67 41 85 25
marie-lise.flottes@lirmm.fr +33 4 67 41 86 35
sophie.dupuis@lirmm.fr +33 4 67 14 97 52

Starting Date / Duration:

Starting: Between October and December 2017
Duration: 3 years

How to apply

1) **Applications can be done from April 27, to Mai 26**. Additional details are provided here:
http://www.adum.fr/script/candidature/index.pl?site=ISS
2) **Fill the on-line application form**:
http://www.adum.fr/as/ed/voirproposition.pl?langue=en&site=ISS&matricule_prop=14624#version
3) Send an email to giorgio.dinatale@lirmm.fr with your CV, a motivation letter and two reference letters
4) Pre-selected applicants will be interview from Mai 30 to June 13
5) On June 21, 2017 we will communicate if you are selected