CentraleSupélec

IETR
INSTITUT D'ÉLECTRONIQUE ET DE TÉLÉCOMMUNICATIONS DE RENNES

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
RENNES

Master Internship in Cybersecurity - Research Position (5 months)

"Circuit Diversification for Improved Security of FPGA Computing Architectures"

Scientific and Technical Context

Cybersecurity has become one of the major concerns in all types of systems, from data centers to edge computing to Internet of Things. Cybersecurity is concerned with different types of system's vulnerabilities that are exposed to attackers. Depending on the attacker's objectives, confidentiality, integrity and availability of the system can be jeopardized. In this broad context, **the proposed internship focuses on the confidentiality of embedded systems**, i.e. on **preventing the leakage of data that could be intercepted by an attacker**. In today's embedded systems, **Side Channel Attacks** (SCA) constitute one of the most critical **vulnerabilities**. Side channels lead to a risk of leaks of sensitive and unencrypted data, known as "red" data, from an information system; the non-sensitive or encrypted data being qualified as "black". SCAs are non-invasive (and often non-detectable) methods that can retrieve red data from a system by exploiting indirect sources of physical information leaked from the device, which include, among others, power consumption and electromagnetic radiation. When trying to access red data, an attacker can exploit any computation-related physical phenomenon and work on recovering data from its correlation to the computational activity. As a consequence, collecting large traces of leaked signals and performing a statistical analysis is often the preferred approach for SCA attacks to find the correlation between leaked traces and red data. Usually, the specific targeted red data is a cyphering key, leading when disclosed to a permanent data leak.

The information leaked by a digital circuit depends on its physical structure, which produces a certain transistor switching activity that results from the computation over red data. Hence, a circuit's architecture, specifically its low-level implementation, is ultimately responsible of its security, as it plays a key linking role mapping inputs to outputs. This is exactly what most SCA-based attacks leverage on looking for this correlation between input data, output data and switching activity. To date, there is no method to assess the inherent security of a circuit according to its architecture implementation. **FPGA** circuit descriptions are contained in the configuration bitstream (a file of bits), which contains the configuration of the underlying Look-Up-Tables, registers and interconnects. Consequently, different FPGA configurations produce different switching activities, and hence the resulting leakages should be different. Viewed from a different angle, two functionally equivalent circuits with different physical implementations that process the same input data, should only differ in their bitstreams and in their *leakage fingerprints*.

Several techniques have been developed to **make cryptographic circuits computation independent of the secret key**, using data hiding or masking to randomize or make the envelop of the leaked information constant. However, not that much work has been done to either: (1) properly understand the relation of a given architecture implementation with its resulting degree of security (resistance to attacks); and (2) consciously build functionally equivalent architectures with different implementations and expected levels of security.

Work Plan

In this general context, the work plan devised for this internship focuses on **understanding how the architecture of cryptographic primitives affects the confidentiality of their data**. On one side, we will explore **innovative FPGA design methodologies and tools** to build functionally equivalent circuits featuring different architectures and physical implementations that intentionally produce different leakage fingerprints. On the other side, we will investigate **analytical and machine learning based methodologies and metrics** that allows **ranking the systems' security.** You will be involved in the following tasks during this internship:

- Build a library of cryptographic primitives with different physical implementations per primitive
- Build complete cyphers with different architectures using the library primitives
- Perform side channel attacks on the built circuits
- Analyze the impact of the different circuits on the resulting side channel leakages (correlation with implementation)
- Devise (quantitative) metrics to assess the "degree of security" of the implemented circuits
- Disseminate your work to the research community by learning how to write a paper with your results

Candidate Profile

- **Master student** (or 5th year Engineering) in: Embedded Systems, Computer/Electrical Engineering, Electronics, Telecommunications Engineering or Computer Science
- Ideally you have **theoretical/practical experience** in one/various of the following topics (and can demonstrate it): *design for FPGAs using VHDL or Verilog; Xilinx FPGAs and design tools; embedded systems architectures; computer/hardware security; Python or C programming*. Please don't hesitate to contact us if you are not sure if your experience could match the profile.

This internship is for you if you can see yourself reflected in at least one of the following: you like to participate in innovative projects with high expected impact; you like system design, programming and/or security; you like research; you are planning to begin a PhD; you would like to write a paper; you would like to work in a high-tech company in hardware security; you have initiative to do your own proposals; you are a proud computer geek.

Please send us:

- Your CV along with your academic records and marks
- A motivational text
- Any additional documents/links that you think can show your experience

Hosting laboratory: IETR (Institute of Electronics and Telecommunications of Rennes)

Hosting institutions: CentraleSupélec

Research groups: SCEE (Signals, Communications and Embedded Electronics) and VAADER (Video Analysis and Architecture Design for Embedded Resources)

Starting date: February/March 2020

Duration: 5 months

Salary: around 580€/month

Contacts:

Rubén SALVADOR: ruben.salvador@centralesupelec.fr
Amor NAFKHA: amor.nafkha@centralesupelec.fr
Maxime PELCAT: Maxime.Pelcat@insa-rennes.fr