Institute of Engineering and Management of Grenoble Alpes University

HR EXCELLENCE IN RESEARCH

Grenoble INP - UGA is a member of **international** engineering and management education and research **networks.** It is widely recognized in national and international rankings**.**

8 schools + **39** laboratories

8300 students

1 300 teaching, research, administrative and technical staff

Grenoble INP - UGA is a renowned public institution of higher education and research, and a major player in the Grenoble ecosystem. It is the engineering and management institute of Grenoble Alpes University, and plays a leading role in the scientific and industrial community.

PhD in Digital Design Engineering

Job ad reference	2024-PHDDIGITALENG-LCIS
Research field	Digital design engineering
Host laboratory	LCIS - Univ. Grenoble Alpes, Grenoble INP Website : https://lcis.fr/
Requested profile	Master / PhD - Degree in Telecommunication, digital design Engineering, or a closely related field in Electronic and Electrical
Location	Valence, France
Hiring date / contract term	01/05/2024 (36 months)
Contacts	romain.siragusa@grenoble-inp.fr

Grenoble INP - UGA is a leading public institution accredited with the French label “Initiative d’excellence”. It offers innovative engineering and management programs, with an increasing internationalization of its course offers. The courses are grounded in sound scientific knowledge and linked to digital, industrial, organizational, environmental and energy transitions. The Engineering and Management Institute of Grenoble Alpes brings together more than 1300 staff members (teacher-researchers, lecturers, administrative and technical staff) and 8300 students, located on 8 sites (Grenoble INP - Ense3, Grenoble INP - Ensimag, Grenoble INP - Esisar, Grenoble INP - Génie industriel GI, Grenoble INP - Pagora, Grenoble INP - Phelma, Polytech Grenoble, Grenoble IAE and the INP Prepa). Grenoble INP is also a highly-ranked institution of higher education and research, leading the way in the fields of engineering and management on an international scale. It is a member of a large number of international academic and research networks. It is part of the European University UNITE!.
As part of Grenoble Alpes University, Grenoble INP has associated guardianship of 39 national and international research laboratories and of technological platforms. The research conducted there benefits both its socio-economic partners and its students. Grenoble INP is at the heart of the following scientific fields: physics, energy, mechanics and materials; digital; micronanoelectronics, embedded systems; industry of the future, production systems, environment; management and business sciences.

Grenoble INP - UGA is an equal opportunity employer committed to sustainability. Grenoble INP-UGA celebrates diversity and equity and is committed to creating an inclusive environment for all employees. All qualified applications will be considered without discrimination of any kind.

Research

LCIS

The LCIS is a public research laboratory associated with Grenoble-INP on the UGA Valence campus of the Université Grenoble Alpes.

The LCIS brings together more than 60 researchers in computer science, electronics and automation, focusing on embedded and communicating systems. Topics covered include the safety and security of embedded and distributed systems, the modeling, analysis and supervision of complex open systems, and communicating wireless radio systems.

The laboratory works on a wide range of applications: Internet of Things, cyber-physical systems, natural or artificial connected environments, RFID, etc.

Job description :

Today's systems are more and more interconnected. Since the advent of the Internet of Things (IoT), any sensor can be interfaced with a local network or the Internet. This massive deployment has created many security issues and associated solutions. The security of the communication can be done thanks to cryptography. However, the complexity of the solution does not necessarily make it compatible with very low-cost systems such as can be found in a sensor network.

Another security flaw studied concerns hardware attacks. Indeed, covert channel analysis, such as power supply analysis, or fault injection attacks, such as sending electromagnetic pulses, can copy the operation of a device in order to add a third-party object in the network or to make it inoperative. These attacks can also disrupt the generation of data encryption keys by attacking the chip's random number generator. To avoid them, it is possible to shield the chips to avoid any radiation or to use error correcting codes. However, solutions are often cumbersome to implement in an IoT device.

The thesis will be part of a European project on the creation of a secure chip for IoT systems. The main objective of the thesis is to design a low speed wireless link without using any analog component and to associate tools to identify an IoT module and to detect hardware attacks in real time during the communication. During the project, these modules will be emulated by RF FPGA boards designed at the beginning of the project. The first objective of the project will therefore be to propose a very low cost wireless link without analog components using simple digital modulation in the ISM frequency bands by simply adding an antenna to the FPGA component. During a previous work, our team showed that it was possible to use FPGA components at RF frequencies (around 600 MHz) to perform OOK (On-Off Keying) wireless links over several meters using an amplifier.

The innovation of this first objective lies in the possibility of operating in ISM bands without any analog components (saving space, cost, consumption). A particular work on the FPGA such as the study of the ring oscillators (RO) used for the carrier will be carried out in order to allow a frequency rise.

The link will then be fully characterized in terms of throughput, range and bit error rate. The second objective is to add functionalities to identify a network module and to detect hardware attacks on it using the developed wireless link. Indeed, the communication carrier signals are generated by ROs. This type of resonator, used in particular in random number generators, have the particularity of being very sensitive to the characteristics of the chip: threshold voltage, supply voltage, temperatures, etc.

Two identical resonators implemented in two different places in an FPGA will therefore have a slightly different frequency. This property has been used to authenticate FPGAs in the Protect project. By using these ROs to communicate, whose frequency will be specific to the device, it is possible to define an identifier associated with its frequency. It will also be possible to detect an attack by monitoring the frequency variations of the oscillators at the reception because they are very sensitive to any variation of the environment. The monitoring module will be developed at the logic level, as close as possible to the hardware. The more we work at low level, the more we will have a fine control on the system. We will work on the number of resonators per module to make the identification and monitoring as reliable as possible.

***Project summary**:*

The thesis is part of a European project KDT JU on the creation of a secure chip for IoT systems.

Main goals:

The main goals are to develop a low cost wireless communication using low frequency FPGA and to define hardware security tools based on this communication.

Keywords : FPGA, Internet of thing, wireless communication, hardware security

Software : FPGA programming in VHLD or Verilog.

Specific requirements or conditions

Position assigned to a restricted area: NO

How to apply

Applications must be sent to : Romain Siragusa : romain.siragusa@grenoble-inp.fr

Application deadline : 24/04/19 April 19th