Call for applications – PhD candidate

IMEP-LaHC,
Grenoble Institute of Technology,
Grenoble-Minatec,
F-38016 Grenoble, FRANCE
https://imep-lahc.grenoble-inp.fr/en

PHOTONIC PHYSICAL UNCLONABLE FUNCTIONS FOR SECURE NEUROMORPHIC PHOTONIC ACCELERATORS

The rising needs of processing information at the edge for low latency, high speeds, and energy efficiency purposes leveraging edge-computing as well as IoT devices (75 billion expected by 2025) for data collection and processing demands for more robust and reliable security layers to guarantee hardware integrity and information security. Security layers are a fundamental part of our hardware and digital infrastructure fulfilling several key functions e.g., assuring that a hardware sub-system is not counterfeit, that a client has authentication rights onto a server or that generated/processed data come from a non-corrupted accelerator. Counterfeiting poses a serious threat to the security of large-scale systems relying on the integration of several sub-systems e.g., counterfeit chips have been found in ballistic missiles and fighter jets. Besides, the massive exchange of sensitive data in the context of edge computing for applications such as autonomous driving, requires that pitfalls shall not be exploited by an attacker to compromise the security of the platform.

The focus of this work will be to develop novel security layers that do not rely on the physical storage of a digital secret key in memory, potentially accessible exploiting SW or HW vulnerabilities. Physical unclonable functions (PUFs) represent a recent class of security layers that can be used for applications in cryptography e.g., end-to-end encryption, blockchain, secure data storage etc. Fabrication tolerances in CMOS platforms guarantee the intrinsic HW unclonable character of such solutions and contribute to the complexity of their behavior for well-designed architectures.

Although electronic PUFs are currently predominant, they have been shown to be vulnerable to machine learning attacks. Conversely, photonic PUFs have demonstrated an increased strength against machine learning attacks due to their richer responses and larger number of physical quantities for key generation e.g., phase, amplitude, polarization as well as superior stability and manifold implementations of optical non-linearities.

In the framework of the Horizon Europe research project NEUROPULS (NEUROmorphic energy-efficient secure accelerators based on Phase change materials aUgmented siLicon photonicS), the PHOTO group at IMEP-LAHC aims to develop novel silicon photonic PUFs for hardware integrity and information security. This work will allow IMEC-LAHC and the other consortium partners involved in security tasks to explore various security protocols at a prototype level (photonic chips will be fabricated by CEA-LETI in a worldwide unique silicon photonics platform with III-V and phase-change materials monolithically integrated) for the next-generation of hardware accelerators based on photonic neuromorphic architectures interfaced with RISC-V core processors to target edge-computing applications.

In this context we are currently looking for a (m/f) **PhD student** for a **3-year** contract.

Job description

This thesis aims to explore novel implementations of photonic PUFs based on CMOS-compatible Silicon Photonics approaches for applications in hardware integrity (identification) and information security (secure authentication, data signature, encryption…).

The work will involve (i) exploring various photonic architectures by means of system-level simulations considering the role of fabrication tolerances on the device modelling, (ii) assessing experimentally the performance of the prototypes (fabrication carried out by CEA-LETI), (iii) carrying out an experimental analysis in terms of robustness and reliability by exploiting techniques well-known in the PUF and reliability communities, and (iv) proposing novel device/system designs and strategies to build more robust and reliable PUFs. The work will involve behavioral and system-level modeling of photonic devices and architectures, robustness and reliability analysis of the designed architectures, and the proposal of novel design/system-level solutions.

Profile

You have or are about to obtain an MSc in Electronic or Physical Engineering with strong experience in at least one of the following areas: analog / digital / photonic integrated circuit design, multi-disciplinary or system-level modelling. Previous experience in design and characterization of photonic devices/systems is a plus. Excellent written and verbal communication skills in English. Fluency in French is also a plus, but not mandatory.

About IMEP-LaHC and PHELMA

The Institut de Microélectronique Electromagnétisme Photonique & LAboratoire d'Hyperfréquences & de Caractérisation, IMEP-LaHC, is a « unité mixte de recherche » (CNRS / Grenoble INP / UGA / Université Savoie Mont Blanc) of 110 people strongly committed in research activities related to micro- and nano-electronics, microphotonics, micro- and nano-systems, microwaves and microwave-photonics. The PHOtonics Terahertz and Optoelectronics (PHOTO) group is a leader in the broad field of photonics and high-speed frequencies, with research projects and collaborations at both national, European, and international level.

Grenoble Institute of Technology (PHELMA school), who issues the PhD degree, is a member of the "*Grandes Écoles*", a prestigious group of French institutions dedicated to engineering and scientific research.

More information about the scientific and industrial environment around Grenoble and its surroundings can be found here: https://www.nature.com/articles/d41586-023-00109-x

Send CV and statement of purpose (in English or French) to

Fabio Pavanello – email: fabio.pavanello@cnrs.fr