Title	Protection of a processor with DIFT against physical attacks
Context	In the age of the Internet of Things (IoT), embedded systems are becoming massively widespread in critical infrastructures such as industry, smart cities, bio-medical devices, etc. They contribute to better control and optimization of infrastructures to increase their efficiency and use, but also to meet societal challenges such as climate change or health. Unfortunately, they also contribute to the increase of the global attack surface of information systems, which represents an unprecedented threat. It is therefore essential to guarantee the best level of protection for such systems, which generally have a low-power processor as their main component. The latter handles sensitive data during security tasks. Due to network connectivity and physical proximity to the attacker, it faces both software and physical attacks. Taking into account simultaneously these two types of attacks during the design of the processor is thus essential although this problem is still insufficiently understood by the scientific community. Indeed, the works published in the literature focus essentially on only one of these types of threat. Moreover, the integration of protections developed to counter software attacks can favor certain physical attacks (for example by increasing the electrical activity linked to certain sensitive instructions). DIFT (Dynamic Information Flow Tracking) techniques allow the detection of various software attacks by attaching and propagating, at runtime, tags to information containers (registers, memory areas, etc.). Combined with an information flow management policy, they can detect violations of the security policy instantiated by the programmer (e.g., access to an unauthorized memory area, transmission of unauthorized data). The proposed topic aims at designing and evaluating a DIFT-like protection mechanism that is robust to physical attacks exploiting auxiliary channels and fault injections. This device will be developed and integrated in an embedded processor taking into account the constraints of circuit area, performance and power consumption. This thesis topic is part of a larger ambition to develop a low-power processor resistant to a wide range of software and hardware attacks. Thus, the ongoing work of Noura Ait Manssour (2019-2022) is part of this ambition and focuses on the protection against certain physical attacks of simple integrity mechanisms of the instruction stream via techniques such as instruction replay. The proposed topic covers another dimension of the problem in order to reach a more global solution. The thesis work will be supervised by Vianney LAPOTRE, Associate Professor, who works in hardware security, and directed by Guy GOGNIAT, Professor, who brings nearly twenty years of experience in the field of embedded systems security. Vianney LAPOTRE is currently co-supervising Noura Ait Manssour's thesis (2019-2022) and Ghita Harcha's thesis, which will be defended in early 2021, on the protection of a hardware AES encryption architecture for IoT against auxiliary channel attacks. Vianney LAPOTRE wishes to defend his Habilitation to Supervise Research towards the end of this thesis. This will allow to reinforce the research activity within the ARCAD team with a greater capacity to supervise works.
Objectives	In view of the significant growth in the number of embedded systems in our daily lives, the development of secure processors is an issue of national and European sovereignty. The RISC-V open source processor architecture offers the opportunity to develop and share original research work on a common basis. It is in this spirit that our work will be based on RISC-V. In this thesis, we will focus on the protection of the information flow within the processor core. We will be particularly interested in fine-grained DIFT mechanisms working on physical information containers: registers, memory areas, input/output interfaces. In order to integrate the protections developed during this work, the micro-architecture of the target processor will be modified and extended in a "secure by design" approach. The proposed protections will be evaluated in terms of performance, circuit area, power consumption and security on FPGA target. For this, we will use the A2C2P2 security evaluation platform of electronic components against physical attacks (developed at the Lab-STICC in Lorient in the framework of the CPER CyberSSI 2015-2020). For the evaluation of protections against software attacks, we will mainly rely on existing benchmarks (e.g. RIPE) and source codes developed during previous projects (Labex HardBlare 2015-2019). This work will take place within the ARCAD team of the Lab-STICC in Lorient which has a strong expertise in the field of hardware security, which will favour interactions with other PhD students and researchers of the laboratory.
Novelty of the project	Among the new countermeasures we wish to study, the issue of secure tag propagation seems central to us, so we will explore the implementation of encoded (for error detection) and masked (for auxiliary channel leakage reduction) tags. Such an approach requires a dedicated arithmetic that we will also study. It is important to note that the attack techniques considered in this project are well mastered within the team and that we also have experience with DIFT techniques. In this work, the proposed solutions will be purely hardware based. Therefore, no modification of the compilation chain is envisaged (except potentially the addition of configuration instructions). The proposed protection mechanisms will be integrated into a RISC-V processor, implemented on an FPGA circuit in order to be able to prototype and evaluate the proposed solutions in terms of performance, power consumption, circuit area and security on the A2C2P2 platform.

International collaboration	In the framework of the thesis we will encourage international mobility. We think for example of the team of Professor Russell Tessier, College of Engineering, University of Massachusetts, Amherst, USA with whom we work regularly. We have other potential partners, we will see the most relevant team according to the contributions we will get.
Expectations	The proposed topic is fully in line with the French and European dynamics around the RISC-V processor. Indeed, the mastery of processor architectures is an issue of sovereignty. This is why communities of researchers and industrialists have organized themselves in order to address the multiple challenges related to RISC-V (IoT, high performance computing, telecommunications, security, etc.). The proposed work is focused on the security of RISC-V processors. Within the French community, various research projects are being carried out on the security of RISC-V processors. For example, the ANR COFFI project (https://anr.fr/Projet-ANR-18-CE39-0003) focuses on resistance to physical fault injection attacks and brings together partners from the CEA, the LIP6 and LabHC laboratories, and the company Invia ISSM. Another remarkable effort of the academic community is the ANR ARCHI-SEC project on the resistance of processors to attacks on the micro-architecture (e.g. Spectre/Meltdown) and gathers partners from LTCI, LIRMM, LabHC, IRISA laboratories and the company Secure-IC. The originality of our topic lies mainly in the design of protection mechanisms against software attacks and against physical attacks. It is thus complementary with the efforts carried out on the national and Breton territory and aims at addressing the fundamental question of security in depth. Indeed, the addition of protection mechanisms can introduce cross vulnerabilities, so it is essential to systematically assess whether a countermeasure for software attacks does not introduce vulnerabilities for physical attacks and vice versa. The work we have been doing for several years on the protection of embedded systems against software and physical attacks allows us to gather the necessary skills to carry out this project.

References

[1] M. Dalton, H. Kannan, and C. Kozyrakis. Raksha: A Flexible Information Flow Architecture for Software Security, in proc. of International Symposium on Computer Architecture (ISCA). 2007.

[2] C. Palmiero, G. Di Guglielmo, L. Lavagno and L. P. Carloni, Design and Implementation of a Dynamic Information Flow Tracking Architecture to Secure a RISCV Core for IoT Applications, in proc. of IEEE High Performance extreme Computing Conference (HPEC), 2018.