INSTITUT D'ÉLECTRONIQUE ET DES TECHNOLOGIES DU NUMÉRIQUE

Fully funded PhD position (3 years, starting Sept./Oct. 2022): **μ-architectural protection of a RISC-V open-hardware processor**

Key words: Hardware security, side-channel attacks, RISC-V, Open Hardware

1 Scientific Context

For decades, processor designers have focused on improving the performance and energy consumption of systems. However, in recent years, it has been proved that attacks directly on the hardware, allow to steal secret information by exploiting vulnerabilities, introduced as side effects, by performance optimization mechanisms [GYLH16, RM13]. Among these, attacks have highlighted security flaws due to the use and sharing of cache memories [GMWM16, IES15], and other μ-architectural components in high performance processors. They typically exploit caches [SGZS21], performance counters [BM18] or speculation units and jeopardize the safety and the of processors in industrial systems. We can cite Spectre [KHF+19] and Meltdown [LSG+18] as well-known examples.

The OpenHW approaches and specifically the RISC-V[1] initiative are now both an economic reality and an innovation opportunity for European actors in the field of processors architecture. This opportunity opens the way to design innovative secure processor cores. In the OpenHW approach, the processor is proposed in the form of a block described in a hardware description language (SystemVerilog in this project) which can be modified according to the requirements of the system.

This PhD position is in the frame of the ANR SecV project starting in March 2022. The originality of the approach lies in the integration of a dynamic code transformation unit, adaptive memory management policies, and a dynamic control unit based on runtime verification, opening the way to numerous online adaptations aiming at supporting the concept of cyber resilience [KL21].

This particular PhD position will focus on μ-architectural-based side-channel attacks, able to gain information on data that would otherwise remain secret, and will investigate the design of innovative secured-by-design open-source processing core against these attacks. The recruited candidate will develop a prototype as demonstrator of the proposed solutions.

2 Scientific issues and objectives

The main objective of this PhD work is to study μ-architectural attacks vulnerabilities and to investigate new defenses to increase the security of the CVA6[2] processing core based on the RISC-V ISA, using the capability of a dynamic control unit. The security strategy implemented in SecV is strongly based on the obfuscation of the micro-architecture behavior, and aims primarily at countering side channel attacks (at least cache and synchronization attacks). This obfuscation relies on the dynamic adaptation capabilities introduced at the instruction decoder and memory hierarchy level, driven by the control unit.

[1] https://riscv.org
[2] https://github.com/openhwgroup/cva6

The main tasks for this work will be:

1. To propose micro-architectural modifications that will benefit from the code transformation unit developed by the partners of the project. As a first study this work will explore alternative cache memories as well as adaptable security-oriented cache management strategies according to the current execution context and suitable security level. This study will also take into account other vulnerabilities induced by integrated high-performance mechanisms.

2. The second objective is to provide the target micro-architecture with a programmable unit in charge of runtime verification which aims to detect the violation of security properties expressed on the behavior of the tasks and/or on the states of the micro-architecture. A suspect behavior could come from strange memory access or from data modifications in the control flow.

3. Implement the proposed security policies and blocks in the CVA6 architecture running on top of an FPGA.

3 Candidate profile

The candidate must be able to demonstrate theoretical/practical knowledge in the areas of computer, architecture and embedded systems design. Additionally, skills in FPGA implementation and HDL are mandatory. Some knowledge or at least interest on C programming and security of electronic devices are of interest in the frame of the project.

Depending on the candidate native language, French or English will be the working language. Knowledge in French is not a prerequisite.

4 PhD context

The consortium of the ANR SecV project includes three academic laboratories (IETR, LS2N, and IMS), and two industrial partners (Thales TRT and Thales INVIA). In this project 2 PhDs, one post-doc and several master students will collaborate on the different topics. The successful candidate will do his/her research in the ASIC team from IETR. The candidate will be administratively registered in Nantes, France.

The ASIC research team from IETR has a recognized expertise in the design of adaptable architectures and in hardware security.

The PhD candidate will be fully integrated (discussions, meetings, seminars) in the SecV project consortium, meetings and will collaborate with the other researchers and PhD/master students within the project. He/She may co-supervise internship students. He/She may have some opportunities for teaching (added to his payroll), if interested.

- **Research Laboratories:** IETR (UMR CNRS 6164)
- **University:** Nantes Université
- **Location:** IETR/Polytech, Nantes, FRANCE
- **Intended starting date:** September or October 2022 (3-year duration)

5 To apply

To apply candidates must provide:

- A CV;
- Academic records and transcripts of Master, or of the last year of Engineer school;
- All additional documents attesting the requested skills and knowledge.

To send to:

- **Prof. Sébastien Pillement**, sebastien.pillement@univ-nantes.fr
- **Dr. Maria Méndez Real**, maria.mendez@univ-nantes.fr

Applications will be considered as they arrive and until there is a successful candidate

References

[BM18] Sarani Bhattacharya and Debdeep Mukhopadhyay. Utilizing performance counters for compromising public key ciphers. *ACM Trans. Priv. Secur.*, 21(1), 2018.

[GMWM16] Daniel Gruss, Clémentine Maurice, Klaus Wagner, and Stefan Mangard. Flush+flush: A fast and stealthy cache attack. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 279–299. Springer, 2016.

[GYLH16] Qian Ge, Yuval Yarom, Frank Li, and Gernot Heiser. Your processor leaks information - and there's nothing you can do about it. *arXiv preprint arXiv:1612.04474*, 2016.

[IES15] Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar. S$a: A shared cache attack that works across cores and defies vm sandboxing – and its application to aes. In *2015 IEEE Symposium on Security and Privacy*, pages 591–604. IEEE, 2015.

[KHF+19] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, et al. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2019.

[KL21] Alexander Kott and Igor Linkov. To improve cyber resilience, measure it. *Computer*, 54(2):80–85, 2021.

[LSG+18] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, et al. Meltdown: Reading kernel memory from user space. In *27th USENIX Security Symposium*, pages 973–990, 2018.

[RM13] Chester Rebeiro and Debdeep Mukhopadhyay. Micro-architectural analysis of time-driven cache attacks: Quest for the ideal implementation. *IEEE Transactions on Computers*, 64(3):778–790, 2013.

[SGZS21] Johanna Sepúlveda, Mathieu Gross, Andreas Zankl, and Georg Sigl. Beyond cache attacks: Exploiting the bus-based communication structure for powerful on-chip microarchitectural attacks. *ACM Transactions on Embedded Computing Systems (TECS)*, 20(2):1–23, 2021.