Implementation of scratchpad memories in order to defeat cache side-channel attacks

1 Introduction and context

Hardware side-channel attacks target specific features of processor architectures in order to steal sensitive information, such as the secret keys of encryption algorithms [1]. In particular, cache side-channel attacks (CSCAs) represent a major threat to modern processor architectures.

Cache side-channel attacks can target both instruction and data caches, at various cache levels depending on the implementation. Cache memories are considered preferential targets for such attacks because of their role as buffers close to the CPU, through which data from all kinds of applications, whether sensitive or not, pass. The implementation of CSCAs relies on the attacker's ability to measure or observe activity on the cache, enabling him to deduce information on memory accesses.

The subject of this Master's internship will focus on timing CSCAs, i.e. attacks that rely on the measurement of execution time to track data stored or not stored in the cache, and thus learn about memory access patterns. Examples include the Prime+Probe [2] and Flush+Reload [3] attacks.

The ANR-funded SEC-V research project brings together a consortium of academic and industrial research laboratories to propose solutions for dynamically securing the architecture of a RISC-V processor core [4]. The attacks considered in this project are in particular CSCAs, and part of the work therefore concerns the implementation of innovative means of securing the core's cache memories.

2 Objectives of the internship

As part of the SEC-V project, we propose to study the security benefits of implementing scratchpad memories [5, 6] in the µ-architecture as a countermeasure against CSCAs. Indeed, scratchpad memories could enable the temporary storage of sensitive data without inducing a loss of performance, as their implementation does not require complex tag-decoding logic to label data. With a view to optimizing performance, these memories are accessed via software requests and therefore offer better performance in terms of energy consumption and are less costly in terms of silicon surface area. The main idea being to avoid buffering sensible data in the cache, using instead the scratchpad memory for this purpose.

The aim of this internship is to study the feasibility of using scratchpads for security purposes, and will focus on the following research objectives:

- Drawing up a bibliography on the use of scratchpad memories.
- Propose a countermeasure to CSCAs based on scratchpad implementation. One of the main difficulty is on the memory management hierarchy between the cache and the scratchpad.
- Modify the architecture of the CVA6 processor core to implement the countermeasure.
- Verify the implementation on an FPGA board and perform verification tests.

3 Consortium Description

The SEC-V project brings together a consortium of researchers and engineers from academic laboratories IETR, LS2N, IRISA and research teams from Thales DIS and TRT.

This internship will be supervised in the IETR laboratory, a member of the SEC-V project, by Professor Sébastien Pillement and PhD student Juliette Pottier. You may be required to collaborate with other consortium stakeholders and take part in associated project meetings.

As integration into the IETR laboratory requires access to a restricted secure area, we ask you to take into account the time required to review your profile if you wish to apply (the process can take up to two months).

4 To apply

Send a detailed CV and your master transcript supporting your application.

- **Pr. Sébastien Pillement**, sebastien.pillement@univ-nantes.fr ,
- **Juliette Pottier**, juliette.pottier@univ-nantes.fr ,

References

[1] Valentin Martinoli. "Secure Processors with respect to Micro Architectural Attacks". PhD thesis. Université Grenoble Alpes, 2023. URL: https://theses.hal.science/tel-04145576/.

[2] D. A. Osvik et al. "Cache Attacks and Countermeasures: The Case of AES". In: *Topics in Cryptology – CT-RSA*. 2006.

[3] Yuval Yarom and Katrina Falkner. "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack". In: *23rd USENIX Security Symposium (USENIX Security 14)* (2014).

[4] J. Pottier et al. "RISC-V Processor Enhanced with a Dynamic micro-Decoder Unit". In: *International Conference on Electronics, Circuits and Systems*. 2024.

[5] I. Puaut and C. Pais. "Scratchpad memories vs locked caches in hard real-time systems: a quantitative comparison". In: *2007 Design, Automation & Test in Europe Conference & Exhibition*. Design, Automation & Test in Europe Conference. 2007. URL: http://ieeexplore.ieee.org/document/4212020/.

[6] A. Singh et al. "SPX64: A Scratchpad Memory for General-purpose Microprocessors". In: *ACM Transactions on Architecture and Code Optimization* (2021). URL: https://dl.acm.org/doi/10.1145/3436730.