TiMA
TECHNIQUES OF INFORMATICS AND MICROELECTRONICS
FOR INTEGRATED SYSTEMS ARCHITECTURE

Internship: Cache Timing Attacks on RISC-V

Context	Data protection is fundamentally important in an increasing number of domains. These properties are usually guaranteed through cryptographic protocols and secure primitives that are implemented, either in hardware or software, on systems of various complexity. The economical and societal challenges push for strong, fast, and robust implementations of these functions, which are implemented with the main goal to optimize overall performance. On the other hand, designers must take care that the implementations may be vulnerable to the implementation attacks. It is well known that side channel attacks, based on the observation of a system, are a major security leak: power consumption, EM emission, and computation time can reveal the data being computed. In this context, cache access timing can leak information on confidential data being processed in a CPU. Attacks based on cache access latency [1,2], have proved that even basic microarchitectural features aiming at improving the overall performance can actually open a side channel where confidential information can be extracted [3]. [1] Page, D.: Theoretical use of cache memory as a cryptanalytic side–channel. Cryptology ePrint Archive, Report 2002/169 (2002). [2] Fournier, J., Tunstall, M. (2006). Cache Based Power Analysis Attacks on AES. In: Batten, L.M., Safavi-Naini, R. (eds) Information Security and Privacy. ACISP 2006. Lecture Notes in Computer Science, vol 4058. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11780656_2 [3] A. Andreou, A. Bogdanov and E. Tischhauser, "Cache timing attacks on recent microarchitectures," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017, pp. 155-155, doi: 10.1109/HST.2017.7951819.
Description	The goal of this internship will be to implement an environment allowing to mount cache timing attacks on simple boards equipped with RISC-V CPUs. More in detail, the intern's activities will consist of: - Set up a platform based on a RISC-V board executing baremetal code - Set up the required flow to perform side channel analysis on the selected board - Develop a proof of concept of the attack exploiting side channel leakage - Study alternative leakage sources - Propose potential countermeasure(s) to protect those features - Validate the countermeasure(s)
Prerequisites	Digital design, RISC-V, embedded development, trace measurements Knowledge of hardware security is a plus

Contacts	Paolo MAISTRI (paolo.maistri@univ-grenoble-alpes.fr)
Applications	Please send your resume, application and recommendation letter(s), first year master's degree grades (mandatory) and second year grades (if possible)
Location	TIMA Laboratory, 46 avenue Félix Viallet, 38000 Grenoble
Starting date	Feb-2024
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 600€/month).

Our team welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as strength and an asset.