A Memory Hierarchy Protected Against Side-Channel Attacks

E. Bertrand Talaki [(1)], Olivier Savry, David Hely, Mathieu Bouvier Des Noes
Univ. Grenoble Alpes, CEA, Leti, F-38000 Grenoble, France; firstname.lastname@cea.fr
[(1)]Poster presenter: ezinam-bertrand.talaki@cea.fr

Description of the poster

In the vulnerability analysis of System on Chips, memory hierarchy is considered among the most valuable element to protect against information theft. Many first-order side-channel attacks have been reported on microarchitectural components from the main memory to the CPU registers. A power consumption based template attack on the interconnection bus has made it possible to recover the HW of the data passing through it and also the HW and HD of the data in the registers of a SoC embedding a RISC-V based 32-bit CPU [1]. Moreover, the possibility of directly retrieving the value of the data was demonstrated in that same work, with a probability of 0.96 for 200 attack traces and a residual enumeration complexity of $2^{13.2}$. Cache memories vulnerability to first-order power analysis attack has also been exhibited [2]. In this context, memory hierarchy encryption is widely used to ensure data confidentiality. Yet, this solution suffers from both memory and area overhead along with performance losses (timing delays), which is especially critical for cache memories that already occupy a large part of the spatial footprint of a processor. In this poster, we propose a secure and lightweight scheme to ensure the data confidentiality through the whole memory hierarchy. This is done by masking the data in cache memories with a lightweight mask generator that provides masks at each clock cycle without having to store them. Only 8-bit Initialization Vectors are stored for each mask value to enable further recomputation of the masks. The overall security of the masking scheme is assessed through a mutual information estimation that helped evaluate the minimum number of attack traces needed to succeed a profiling side-channel attack to 592K traces in the attacking phase, which provides an acceptable security level with the condition of having a Signal to Noise Ratio of 0.02. The lightweight aspect of the generator has been confirmed by a hardware implementation on Digilent Genesys 2 FPGA that led to resource utilization of 400 LUTs with a maximum working frequency of 150 MHz. Figure 1 illustrates the protected memory hierarchy that will be implemented on a 64-bit RISC-V based SoC. Instead of sending encrypted data in the caches, we decrypt it at the output of the interconnect bus and mask it before sending it to the last level cache. At the output of the L1 cache, the masked data and the mask are sent to the registers. This provides inputs for the execute stage to process instructions on masked data.

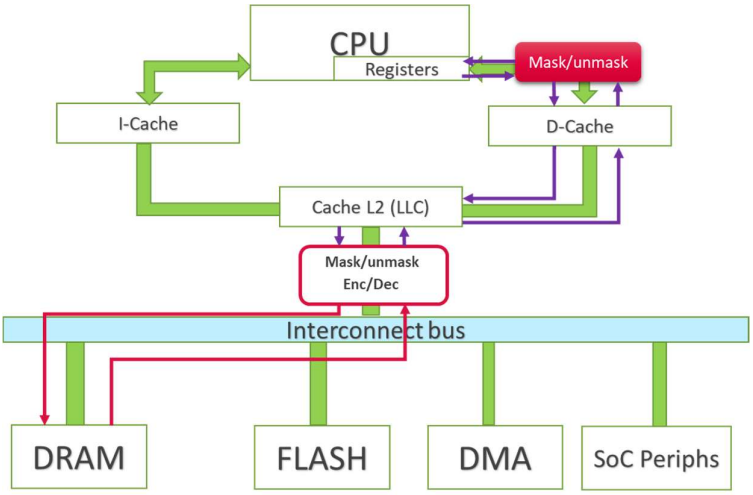

Figure 1 Protected memory hierarchy.

References

[1] E. B. Talaki, M. B. Des Noes, O. Savry, D. Hely, S. Bacles-Min, et R. Lemaire, « Exposing Data Value On a Risc-V Based SoC », in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, p. 1–8.

[2] R. Giterman, O. Keren, et A. Fish, « A 7T security oriented SRAM bitcell », *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 66, nº 8, p. 1396–1400, 2018.