FRANÇAIS ENGLISH

cea leti

ScrambleCache

PATENTS 2 PATENTS

Enhanced security for processors cache memories

What is ScrambleCache?

Cache memories reduce the access time between the main memory and the processor. They are vulnerable to cache timing attacks, which can be used to obtain sensitive data or encryption keys.
ScrambleCache is a hardware countermeasure that improves the two most commonly used security mechanisms: randomization and cache partitioning.
Its efficiency was proven by using a write-through cache memory. It was demonstrated using FPGA with the RISC-V CVA6 processor and two patents were filed.

Applications

ScrambleCache is suitable for all processors that use cache memory, especially those found in:

- Personal and professional computers
- Smartphones
- Automobile ECUs
- Medical devices
- Industrial electronics

These devices manage sensitive data and can be subject to targeted attacks through software side-channel attacks also called cache timing attacks.

Work performed in the frame of the IRT Nanoelec consortium.

NANOELEC.

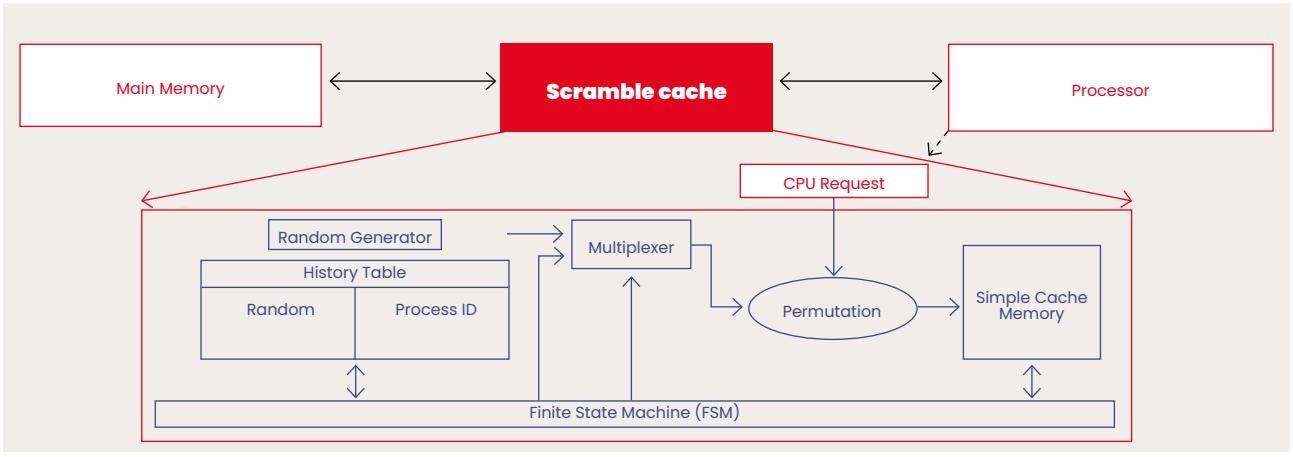
What's new?

While randomization and partitioning help protect cache memories, they also slow down processors. ScrambleCache reduces this latency:

- **Thanks to randomization** (i.e. adding pseudo-random variables that bias an attacker's observation of memory access times): adds a randomization history table and associated application identifiers in order to avoid routinely clearing and reloading the cache.
- **Thanks to partitioning** (i.e. the distribution of data in various areas of memory): uses dynamic and therefore variable partitioning as well as a check of legitimacy for each application on every piece of data. This reduces the need to reload data that is shared by several applications.

Publication

A. Jaamoum, T. Hiscock, G. Di Natale "Scramble Cache : An Efficient Cache Architecture for Randomized Set Permutation", DATE Conference 2021



What's next ?

- Optimize ScrambleCache for write-back cache and evaluate it on ASIC.
- Benchmark ScrambleCache with various Linux OS applications to confirm its reduced impact on access times (already demonstrated through simulation).
- Study the implementation of ScrambleCache on different types of processors.

Interested in this technology?

Contact:
Marion Andrillat
marion.andrillat@cea.fr
+33 (0) 438 784 651

CEA-Leti, technology research institute
17 avenue des Martyrs, 38054 Grenoble Cedex 9, France
cea-leti.com

@CEA-Leti

Research for industrial innovation