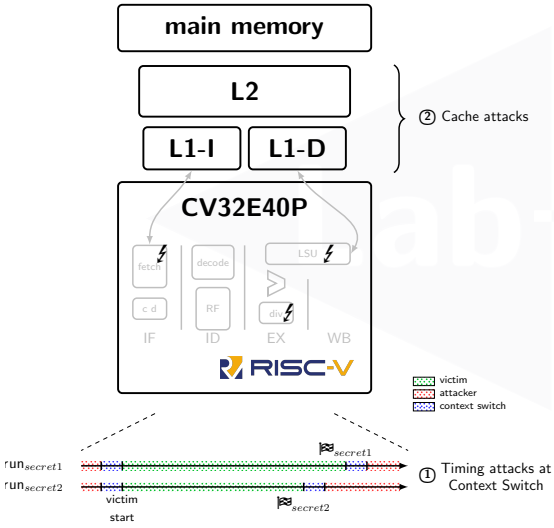
Verrouillage de lignes de cache pour la lutte contre les attaques par canaux auxillaires exploitant les mémoires caches

Nicolas GAUDIN, Vianney LAPÔTRE, Pascal COTRET & Guy GOGNIAT
Lab-STICC, UMR 6285, Lorient, Bretagne, France
contact : nicolas.gaudin@univ-ubs.fr

5 mars 2024

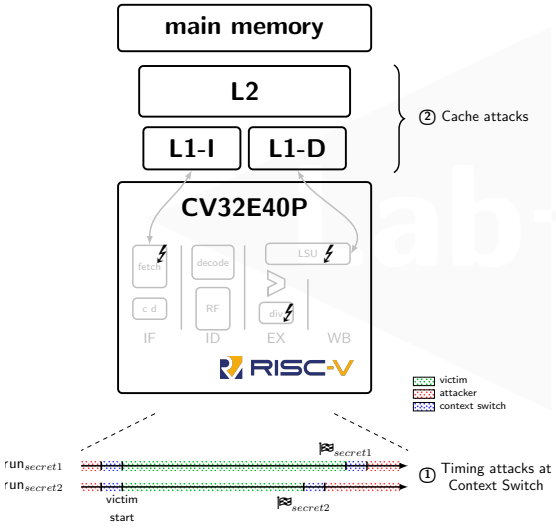
Motivations



and processes are concurrently executing the processor.

only considers timing side channel.

Motivations

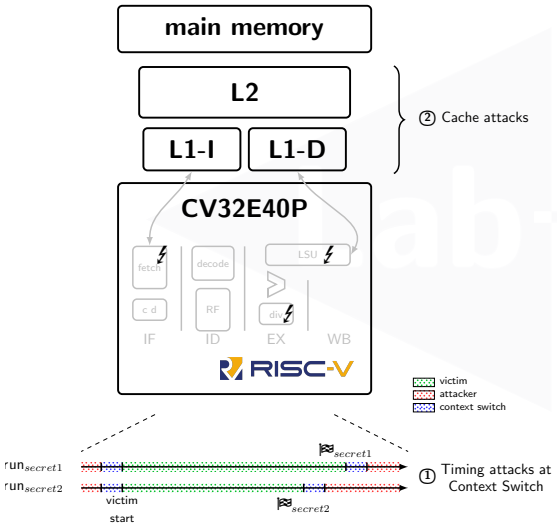


and processes are concurrently executing the processor.
only considers timing side channel.

Ensure **efficient** and **on-demand** constant-time execution

---

Motivations



and processes are concurrently executing the processor.
only considers timing side channel.

Ensure **efficient** and **on-demand** constant-time execution

---

Sources of leakages :

Branching
if (condition(**secret**))

Operation with variable execution time
dividend/**secret** ;

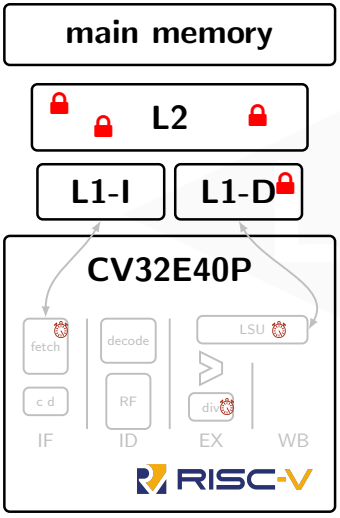
Index for Memory access
array[**secret**] ;

Some Cache Architectures Thwarting Cache-based SCAs

- **RPcache** [1], **ScatterCache** [2] and **Ceaser** [3] propose cache designs based on randomization.
  - ⚠ **P**rime+**P**rune+**P**robe [4] find eviction sets in randomized caches from only hundred accesses.
- **NoMo-cache** [5], **SecDCP** [6], **PLcache** [1] partition the cache.
  - ⚠ Partitioning-based caches imply a performance decrease depending the partitioning granularity.

1. Wang et Lee, "New Cache Designs for Thwarting Software Cache-Based Side Channel Attacks", 2007
2. Werner et al., "ScatterCache : Thwarting Cache Attacks via Cache Set Randomization", 2019
3. Qureshi, "CEASER : Mitigating Conflict-Based Cache Attacks via Encrypted-Address and Remapping", 2018
4. Purnal et al., "Systematic Analysis of Randomization-based Protected Cache Architectures", 2021
5. Domnitser et al., "Non-Monopolizable Caches : Low-Complexity Mitigation of Cache Side Channel Attacks", 2012
6. Wang et al., "SecDCP : Secure dynamic cache partitioning for efficient timing channel protection", 2016

Our `lock` mechanism



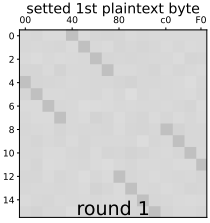
- Extend the Instruction Set Architecture
  - `lock` and `unlock` instructions

🔒 `lock` instr. keeps data cache line in cache
  - guarantee constant time access
  - locked cache line cannot be evicted

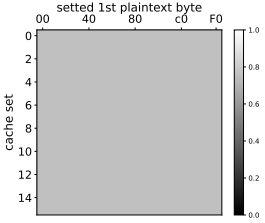
🔓 `unlock` instr. releases locked cache line
  - data can be evicted from now

Results

Security wise



Unprotected execution



`lock` execution

Prime+Probe on AES-128 (1st round only, 1st plaintext byte settled, 300 executions, key = 0x42)

Performance wise

- hardware overhead $< 3\%$
- binary size overhead $< 0.5\%$
- performance overhead
  - $< 3\%$ for AES encr.
  - $< 1\%$ for 4 consecutive AES encr.
- degradation on concurrent processes
  - negligible for AES

Verrouillage de lignes de cache pour la lutte contre les attaques par canaux auxillaires exploitant les mémoires caches

Nicolas GAUDIN, Vianney LAPÔTRE, Pascal COTRET & Guy GOGNIAT
Lab-STICC, UMR 6285, Lorient, Bretagne, France
contact : nicolas.gaudin@univ-ubs.fr

5 mars 2024

Bibliography

- Domnitser, Leonid et al. "Non-Monopolizable Caches : Low-Complexity Mitigation of Cache Side Channel Attacks". In : *ACM Transactions on Architecture and Code Optimization* (jan. 2012). doi : 10.1145/2086696.2086714.
- Purnal, Antoon et al. "Systematic Analysis of Randomization-based Protected Cache Architectures". In : *Proc. IEEE Symposium on Security and Privacy (SP)*. Mai 2021. doi : 10.1109/SP40001.2021.00011.
- Qureshi, Moinuddin K. "CEASER : Mitigating Conflict-Based Cache Attacks via Encrypted-Address and Remapping". In : *Proc. International Symposium on Microarchitecture (MICRO)*. 2018. doi : 10.1109/MICRO.2018.00068.
- Wang, Yao et al. "SecDCP : Secure dynamic cache partitioning for efficient timing channel protection". In : *53ndDesign Automation Conference (DAC)*. 2016. doi : 10.1145/2897937.2898086.

Bibliography

- Wang, Zhenghong et Ruby B. Lee. “New Cache Designs for Thwarting Software Cache-Based Side Channel Attacks”. In : *Proc. International Symposium on Computer Architecture (ISCA)*. 2007. doi : 10.1145/1250662.1250723.
- Werner, Mario et al. “ScatterCache : Thwarting Cache Attacks via Cache Set Randomization”. In : *Proc. 28th USENIX Security Symposium (USENIX Security)*. 2019. url : https://www.usenix.org/conference/usenixsecurity19/presentation/werner.