Enforcing RISC-V TEE Security Against Cache Timing Attacks

Oussama Elmnaouri[1], Pascal Cotret[1], Vianney Lapôtre[2], and Loïc Lagadec[1]

[1]Lab-STICC, UMR CNRS 6285, ENSTA (29806 Brest Cedex 9, France), firstname.lastname@ensta.fr
[2]Lab-STICC, UMR CNRS 6285, Université de Bretagne-Sud (56100 Lorient, France), vianney.lapotre@univ-ubs.fr

Confidential computing includes various methods to enhance data security, notably by processing sensitive information within Trusted Execution Environments (TEEs). However, TEEs remain vulnerable to Side-Channel Attacks (SCAs), such as cache timing attacks, which exploit timing variations to extract confidential data. Existing TEE designs do not provide sufficient protection against these threats, highlighting the need for stronger security measures. This study focuses on integrating countermeasures specifically targeting timing and cache vulnerabilities within a TEE. The implementation will leverage the RISC-V architecture to explore its potential in mitigating SCA within TEE.