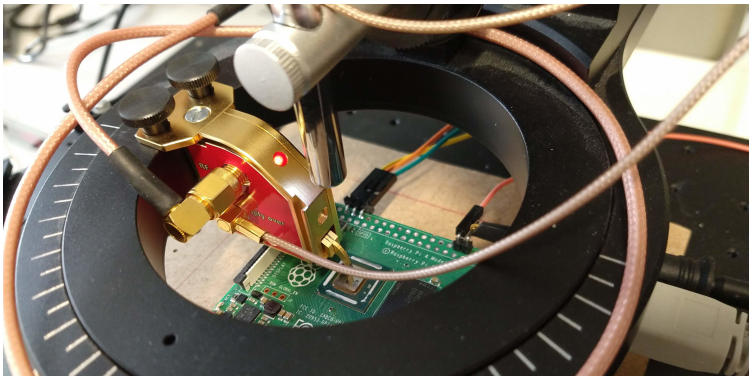
Let's Get Physical: Attacking Real-World Implementations



Processors are becoming increasingly complex. Superscalar, our-of-order architectures allows chip to squeeze the most performance out of their transistors. Yet, most research into physical side-channel and fault attacks is performed on simple microcontrollers operating at a much lower frequency. These threats do, however, still exist on high-end CPUs. These attacks are especially relevant in the context of trusted execution environments such as Intel SGX, and their interplay with the more newly discovered microarchitectural attacks is not yet deeply understood.

In this thesis, you will gain hands-on experience by performing physical attacks on a high-end CPU with various micro-architectural optimizations and a TEE. The main targets will be the Intel-based Hackboard 2, or the Arm-based Raspberry Pi 4. The practical work will consist of a profiling stage where the student investigates the susceptibility of the target platform to physical attacks followed by an actual exploitation of the vulnerability. The device can be either attacked through active methods such as laser fault injection or passively with EM side channels.

Together with the supervisors, students can customize their thesis based on their background and interests. Possible contributions to the field include:

- Application of fault injection techniques to a modern Intel CPU
- Combining physical side-channels with transient execution attacks

The thesis has a fairly strong focus on practical work. The student will have to become familiar with the lab equipment and/or be comfortable writing code to trigger the targeted microarchitectural features. During the thesis, the student will have the chance to work in COSIC's state-of-the-art lab, equipped to perform a wide range of physical attacks such as side-channel analysis, EM fault injection and laser fault injection. Because of the multiple possible research directions for this topic, it is strongly encouraged to contact us before making commitments.

Practicalities

Promotor:	Ingrid Verbauwhede		
Daily supervisor:	Jesse De Meulemeester	jesse.demeulemeester@esat.kuleuven.be	office 01.21
	pcy Sluys	pcy.sluys@esat.kuleuven.be	office 01.20
	Lennert Wouters	lennert.wouters@esat.kuleuven.be	office 01.16

Nature of the work:	25% literature, 75% applied work
Number of students:	1 or 2

 © 2026 – 2027 COSIC