RISC-V is a popular modern open-source CPU architecture. One of its implementations, IBEX, proposes a set of security features, one of which is 'dummy instruction insertion'. This feature serves two goals. It prevents from attacks that extract information from execution timing, and it hinders synchronization required to mount other attacks, such as power analysis. The goal of this project is investigation and potentially an enhancement of effectiveness of this feature against real attacks.

In the course of this project, the students will use simulation to apply attacks on an IBEX rtl model. They will measure the effectiveness by comparing the success rate of the attack with and without the 'dummy instruction insertion' feature and getting quantitative results, such as number of attempts. They will also try to 'learn' the instruction insertion pattern by using various learning techniques. Finally, the students will propose how to improve the protection.

During this project, the students will acquire skills in RTL simulation, CPU testing and some attack techniques on integrated circuits. Students may also choose to employ machine learning techniques for the attacks.