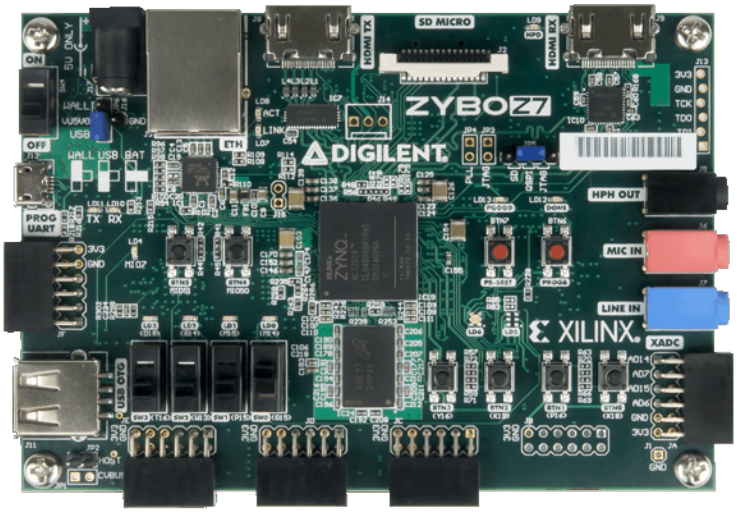
Fuzzing of FPGA Architectures



Field programmable gate arrays (FPGAs) are integrated circuits providing reconfigurable hardware. They are used in a variety of important applications, from ASIC prototyping over accelerating AI workloads to various military applications.

While FPGAs afford a user a degree of control and verifiability over the hardware implemented *on* said FPGA (as opposed to an ASIC), verifying whether the FPGA fabric itself is implemented as advertised is another matter. Typically, fuzzing techniques are used to discover and map the internal architecture of an FPGA.

However, these fuzzing techniques are still at their infancy, and have only been used on a limited set of FPGAs.

The thesis has a fairly strong focus on practical work. The student will have to become familiar with fuzzing techniques, digital hardware design, and algorithms used in place-and-route tools (such as graph theoretical algorithms, optimization techniques such as simulated annealing, and SAT solvers). Because of the multiple possible research directions for this topic, it is strongly encouraged to contact us before making commitments.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Jakob Heirweigh	jakob.heirweigh@esat.kuleuven.be	office B01.24
	pcy Sluys	pcy.sluys@esat.kuleuven.be	office 01.20
Nature of the work:	25% literature, 75% applied work		
Number of students:	1 or 2		

 © 2026 – 2027 COSIC