Improving the Effectiveness of Fuzz Testing by Incorporating Association Rule Mining for Hardware Verification

Abstract:

In the field of hardware design, ensuring the correctness and reliability of designs is crucial for achieving optimal performance and functionality. Functional verification ensures that a system's design meets its specification before manufacturing, by identifying and rectifying design errors. Among the various methods for ensuring system correctness, Assertion-Based Verification (ABV) has emerged as one of the most promising solutions for verifying design functionality. Conversely, testing methods like fuzz testing play a crucial role in pinpointing design flaws and errors. Fuzzing techniques identify flaws in the design by providing unexpected test input to the design and monitoring unusual outcomes, such as crashes and failures. During fuzz testing, a substantial volume of input data is generated and crashes are observed. This data is often voluminous and complex, rendering the testing process time-consuming and costly. Given the limitations of current fuzzers, there is a pressing need to enhance the effectiveness of these techniques to address the increasing complexity of modern hardware designs.

Project description:

The primary objective of this research internship is to enhance the effectiveness of fuzz testing methods for hardware design verification and testing by integrating association rule mining techniques. In this research, our goal is to introduce a novel fuzzer capable of serving as both a testing and verification method for hardware designs. By leveraging data mining approaches, we aim to improve the identification and prioritization of test cases, leading to a more targeted fuzzing process. Additionally, our purpose is to improve the efficiency of the verification process and increase the design behavior coverage of the hardware designs using assertions generated with the proposed fuzzer. In this internship, you will gain in-depth knowledge about the testing, verification, and security of hardware designs. Additionally, you will explore how AI-based techniques, including data mining and machine learning, can be applied to enhance these processes.

Tasks of the internship:

- Installing hardware fuzzers and testing several hardware design benchmarks implemented in the Verilog and SystemVerilog assertion languages.

- Implementing data mining and machine learning techniques for analyzing patterns in the input test vectors of the fuzzers.

- Injecting faults, and Hardware Trojans to the benchmarks and analyzing the experimental results.

Scientific environment:

The candidate will work within the TIMA Laboratory (https://tima.univ-grenoble-alpes.fr/) in collaboration with the AMfoRS (Architectures and Methods for Resilient Systems) research group.

Profile & requested skills:

We are looking for a highly motivated Engineering School or M2 Master's student. Applicants must hold a Master 1 degree (or equivalent) obtained within the last three years at the application deadline, in a related field such as computer science, microelectronics technologies, hardware verification and formal methods, or emerging advances in Artificial Intelligence. Interpersonal skills, dynamism, rigor, and teamwork abilities will be highly valued. Candidates should be fluent in English and have strong English writing skills.

Allowance: Internship allowance will be provided.

Application instructions:

If you are interested in the topic please send your complete application to: mohammadreza.heidari-iman@univ-grenoble-alpes.fr.

A complete application consists of:

Cover letter: A brief motivation statement by the applicant, explaining their connection to the position, how the position aligns with their background, and how it supports their future career goals (maximum 1 page).

CV: Academic and professional background, detailing relevant experience, particularly research.

Relevance for Application: The applicant should include a clear description of how his or her scholarly background and expertise apply to the project outlined above and how they might add value to it.
Our laboratory welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as a strength and an asset.
Depending on the student's motivation, the internship may lead to a doctoral project.

Contact:

Mohammad Reza Heidari Iman,
Postdoctoral Researcher at TIMA Laboratory,
Université Grenoble Alpes,
Grenoble, France
Email: mohammadreza.heidari-iman@univ-grenoble-alpes.fr