Date: 7 July 2020

Time: 11:00 AM

Location: https://meet.google.com/mgu-otvt-sqi

Title: Formal Verification and Security Analysis of High-level Synthesis

Abstract:

High-level synthesis (HLS) is the process of translating high-level languages written in C/C++ into Register Transfer Level (RTL) design. HLS tools are large and complex programs that may be incorrect in some contexts, which might introduce bugs in the generated RTL. Translation validation is the process of proving that the target code is a correct translation of the source program being compiled. In this thesis, a translation validation method based on the propagation of mismatch values in a path based equivalence checking method (PBEC) framework is proposed to validate the various scheduling optimizations during HLS efficiently. Specifically, this method verifies code motion involving loops, ignores the false computations, and handles the scenarios involving path merge/split. We have analyzed the correctness and complexity of the method. Experiments on various HLS benchmarks demonstrate the efficiency and scalability of our method.

In the case of non-equivalence, PBEC approaches provide too little information to debug the root cause of the non-equivalence. This thesis presents a counter-example generation framework to demonstrate the non-equivalence between the input behavior to HLS and the scheduled behavior generated by HLS. The equivalence checking of programs is an undecidable problem in general. Therefore, a PBEC method may produce false-negative results for which the counter-example will not arise. However, this helps the verification engineer to identify the limitation of the current translation validation tool and hence its enhancement in the future.

Logic locking is an Intellectual Property (IP) protection technique against IP piracy, reverse engineering, hardware Trojans, and counterfeiting attacks. RTL locking during HLS seeks to prevent IP theft of a design by locking the RTL description that functions correctly on the application of a key. This thesis introduces a satisfiability modulo theories (SMT) attack to determine the secret key of a locked RTL design. We have shown that our tool can detect keys of a locked RTL generated by TAO, a state-of-the-art HLS locking solution.

Bio:

Ramanuj Chouksey received his B.E. degree in Computer Science & Engineering from SATI Vidisha, Madhya Pradesh, India. He completed his M.Tech degree in Computer Science & Engineering from IIT Guwahati. His PhD thesis, also submitted to the Department of Computer Science & Engineering at IIT Guwahati studies verification and security analysis of high-level synthesis. His research interests are in the area of formal verification, specifically model checking and symbolic execution.