DATE: January 8th, 2021

Department of Electrical and Electronic Information Engineering		ID	M173266
Name	Shotaro Yamada		

Supervisor	Shuichi Ichikawa

Abstract

Title	Evaluation of obfuscation measures for hardware obfuscation

The protection of intellectual properties (IPs) of logic circuits is an important issue. One of the countermeasures is logic obfuscation, which complicates the internal structures of logic circuits to prevent reverse engineering. Direct obfuscation of logic circuits at gate level poses problems such as dependency on specific platforms or changes in timing characteristics. Matsuoka et al. suggested that the use of high-level synthesis (HLS) with generic software obfuscation tools greatly reduces the required effort for obfuscating hardware. HLS is a design method that generates logic circuits from algorithm-level descriptions such as C program. The previous works on hardware obfuscation using HLS confirmed only the increments in latency and logic area. However, it was not quantitatively evident whether the generated circuits are more complex than plain circuits.

This research defines obfuscation measures to quantitatively evaluate the complexity of obfuscated hardware. We generated obfuscated hardware by combining software obfuscation tool Obfuscator LLVM (OLLVM) and high-level synthesis (HLS) tool LegUp.

We obfuscated and converted benchmark programs into obfuscated circuits to evaluate the obfuscation measures. Software-level evaluation targetting at LLVM IR (Intermediate Representation) and hardware-level evaluation targetting at synthesized netlists are conducted. We used CHStone, which is an HLS benchmark suite composed of 12 programs that can be high-level synthesized. OLLVM implements the following obfuscation methods: bogus control flow (B), control flow flattening (F), and instruction substitution (S). Each of the three methods was applied separately.

In the software-level evaluation, we measured the obfuscated IRs and HLS-preprocessed IRs. For each obfuscation method, we calculated eight obfuscation measures. Excluding some metrics that may have measured the increase in logic area rather than the increase in complexity, the maximum increase rates were (B) 111.5%, (F) 320.4%, and (S) 102.8%. Also, it was observed that some metrics were decreased by HLS-preprocessing including optimizations, which explains the cancellation of obfuscation.

In the hardware-level evaluation, we measured the synthesized netlists, the design data for logic circuits. We calculated three obfuscation measures, and the maximum increase rates were (B) 3.61%, (F) 23.5%, and (S) 4.15%, excluding some metrics that may have measured the increase in logic area.

Although we were able to confirm that obfuscation increased the complexity of the circuits, it is necessary to evaluate the relationship between the change in complexity and the actual difficulty of reverse engineering in the future.