DATE: 2021/1/8

Department of Electrical and Electronic Information Engineering		ID	M173237
Name	Masaaki Takeda		

Supervisor	Shuichi Ichikawa

Abstract

Title	Experimental evaluation of Logic Locking method implemented by high-level synthesis

In recent years, with the advance of manufacturing technology for large-scale integrated circuits, the semicondector companies have been specialized in either circuit design or manufacfuring. Companies specializing in circuit design can be exposed to the threat of plagiarism because such companies outsource the manufacturing. Therefore logical encryption techniques that obfuscate netlists of logic circuits have been proposed to protect the intellectual property such as circuit deisgn. Logic locking is an encryption technique to prevent unauthorizied use of logic circuit. The circuit operates correctly only when the key of Logic Locking is correct. Though many of logic locking is implemented for netlist level, the source-level implementation is desired for higher usability.

This study examines SFLL-HD, which is a logic-locking tequnique proposed by Yasin (2019), and simulated and implemented for three applications (DFSIN, JPEG, AES) of CHStone benchmark. In each application, the function having int type argument and return value is target of locking. In the simulation, the mismatch of output signals were examined when incorrect key was used. Output damage was evaluated based on the percentage of incorrect output compared to the expected correct output. Input data is the validation data used in CHStone benchmark. Keys was 32 bits and prepared 5 sets. The Hamming distance was varied from 0 to 32. With this implementation, the overheads of resource and latency of logic locking was evaluated using Xilinx Vivado HLS 2020.1.

In the simulation of DFSIN the largest mismatch of output for each key was 59.4% when the Hamming distance was 14. For JPEG it was 85.8% when the Hamming distance was 17, and for AES it was 100% when the Hamming distance was 13, 14, 15, 18, 19 and 20. From these results, it is confirmed that the output mismatch varies greatly depending on the combination of input data characteristics and keys when SFLL-HD is used. Implementation results showed an increase in the number of FFs and LUTs, which are 0.826% for FFs and 3.57% for LUTs in DFSIN, 6.05% for FFs and 20.0% for LUTs in JPEG, and 11.2% for FFs and 21.8% for LUTs in AES. The maximum latency overhead was 2.48% for DFSIN, 2.95% for JPEG, and 13.9% for AES. The resource and latency overheads were found to be dependent on the number of locations where the locking function was used.