DATE: 2017/1/10

Department of Electrical and Electronic Information Engineering		ID	133242
Name	Kiyohiro Sato		

Supervisor	Shuichi Ichikawa Naoki Fujieda

Abstract

Title	Tamper resistance of the Instruction Register File with Positional registers

Recently, the importance of the defense of embedded software against analysis, plagiarism, and falsification, has been increasing. For example, if embedded software has no countermeasures against analysis, it can be easily disassembled according to its instruction set architecture.

Instruction set randomization (ISR) is one of the obfuscation techniques for embedded software by modifying or enhancing instruction coding system. Hines *et al.* proposed an Instruction Register File (IRF) and a positional register. The IRF is a table of frequently executed instructions. Positional register is a table of register numbers of previously executed instructions. Though they were originally proposed to reduce power consumption by decreasing code size, Fujieda *et al.* proposed to use IRF for the sake of tamper resistance.

This study examines the tamper resistance of the IRF that integrates a positional register. When positional register is applied, a problem arises to decide whether an instruction expression is modified to use the positional register. Another problem is which expression should be chosen from possible candidates. A greedy algorithm is proposed to select the most frequency executed expression from them. Another algorithm is examined for comparison, where as many instructions as possible are modified and expressions are chosen with fixed priority. Two designs of positional register are examined, *field-based* and *usage-based*, which differ in the way to record register numbers. *Field-based* design records the register numbers according to their fields i.e. rs, rt, and rd. *Usage-based* design records them according to their purposes, which are divided into source registers and a destination register.

According to our evaluation, when expressions were chosen with fixed priority, the measure of tamper resistance was reduced by up to 6.7 % with the positional register. When the proposed greedy algorithm was applied, the measure of tamper resistance was improved by up to 6.6 % with the positional register. This increase of the tamper resistance is equivalent to adding 256 entries to a 1024-entry IRF without a positional register.