平成 27 年 1 月 8 日

情報・知能工学専攻	学籍番号	113708
申請者氏名	宇山 和輝	

指導教員氏名	市川 周一 藤枝 直輝

論 文 要 旨(修士)

論文題目	A Method to Protect Control Logic in the Hardware Implementation of PLC Instructions (PLC 命令列のハードウェア化と制御論理保護の一手法)

Control logic of industrial machinery is important intellectual property, which must be protected against various illegal uses. This study describes a method to convert the instruction sequence of programmable logic controllers (PLCs) into the logic circuit of Field Programmable Gate Array (FPGA) that is obfuscated to prevent analyses of the control logic.

Obfuscation is a technique to convert a program or a circuit into a functionally equivalent one that has a complicated architecture or behavior. In this study, obfuscation is applied when the hardware description is generated from PLC instructions. Since PLC instructions include many conditional branches, *opaque predicates* were employed to complicate the branches.

Opaque predicates add conditional branches, which are never executed or never affect the output. Since the conditional expression is a key to obstruct analyses, this study adopted the method based on directed graphs proposed by Collberg.

On the generation of the hardware corresponding to PLC instructions, a new *if-else* statement is inserted in the original *if* statement which corresponds to the condition for PLC instructions to be executed. The condition part of the new *if* statement is designed to return constant value. If the condition becomes true, for example, the *then* part is always executed. The original processes are put in the *then* part, while arbitrary statements can appear in the *else* part for obfuscation.

Two short PLC programs were examined to evaluate the proposed method. Program 1 has a quite small number of PLC instructions, which is used to see if the arithmetic core and the peripheral circuit corresponding to the additional statements are generated. Program 2 is a part of a practical PLC program to evaluate the circuit complexity with the new statements. Logic scale, total fan-outs, and fan-out per logic scale are used as the measures of complexity.

According to our experimental result of Program 1, the logic scales were increased and the operating frequencies were decreased. It suggests that the proposed technique is applicable to the hardware converted from PLC instructions. In the experimental results of Program 2, two different tendencies were observed depending on the additional statements. If the additional statements had different destinations than the original, the logic scale was increased by 30% and the total fan-out was increased by 20% at a maximum; otherwise, the respective increases of logic scale and the total fan-out were l 3.5% and 1.5% at most. These increases of the logic scale and the total fan-outs imply the effect of circuit complication. The fan-out per logic scale decreased in both cases, while the decrease was smaller in the latter case. This result implies that an effective obfuscation can be achieved by adding new statements that have the same destinations as the original statements.