

|             |       |      |         |        |                |
|-------------|-------|------|---------|--------|----------------|
| 電気・電子情報工学専攻 |       | 学籍番号 | M133205 | 指導教員氏名 | 市川 周一<br>藤枝 直輝 |
| 申請者氏名       | 石垣 良樹 |      |         |        |                |

## 論文要旨（修士）

|      |                            |
|------|----------------------------|
| 論文題目 | PLC 命令列の高位合成によるハードウェア化と難読化 |
|------|----------------------------|

知的財産保護のため、プログラマブルロジックコントローラ（PLC）の命令列を保護・隠蔽する技術が求められている。PLC 命令列のハードウェア化・難読化はその 1 つである。本研究では高位合成によって PLC 命令列をハードウェア化・難読化しコプロセッサとした。高位合成の中間言語には C 言語を採用し、PLC 命令列から C 言語の変換には専用コンバータを、C 言語からハードウェア記述言語 (HDL) への変換には商用の高位合成ツール Vivado HLS を用いた。システムは Xilinx Zynq SoC が搭載された Digilent ZedBoard に実装し評価を行った。PLC コプロセッサはソフトウェアから呼び出すことを前提として構築したシステムに組み込んだ。難読化手法には Collberg らが提案した Opaque Predicates を使用した。

Vivado HLS は指示句・オプションを与えることによって生成する回路を制御可能である。田中 (2016) は市川ら (2011) の提案した PLC 命令列のハードウェア化デザインを HLS の指示句・オプションによって再現できるか検討した。本研究ではプロセッサとのデータ転送を考慮したシステム上で、更に多くの指示句・オプションについて検討評価を行った。結果、本研究で構築したシステムで指示句・オプションにより再現可能であるのは、PLC 命令列を並列実行し実行時間の短縮を行う Levelized Design (LD) だけであった。よりよい LD を目指していくつかの指示句を組み合わせた回路を生成し、指示句なしの回路と比較した。その結果、実行時間はパイプライン化によって最大で 2 % 減少し、回路規模は演算器共有によって最大で 44 % 減少した。実行時間のデザインの差はデータ転送時間に隠蔽されたことによってほとんどみられなかった。秋中が作成した PLC システムと回路規模・実行時間を比較した。結果、先行研究と遜色ないものが高位合成によっても作成できていることがわかった。

難読化は宇山 (2015) が実装した Opaque Predicates の枠組みを参考に高位合成環境で再現を行った。これは分岐条件に強連結グラフを用いることで解析を困難にするものであり、偽の分岐先には偽の PLC 命令を使用するものである。宇山はオペランドと命令種の両方の変更を行ったが、本研究ではオペランドは変更せず命令種を変更するのみとした。結果、実行時間は難読化前から 1% の増加にとどまった。回路規模は最大で 2.5 倍に増大し、その増加率は元の回路の回路規模に依存した。回路規模の増加率は難読化元の回路の回路規模のサイズに依存し、使用した 3 つの PLC 命令列のうち最大のものは、資源制約をしなければ廉価な評価ボードである ZedBoard 上に実装できないほど回路規模が増大した。回路規模の増加率は宇山のものより大きい。難読化の特性は同様の結果となり、高位合成環境によっても Opaque Predicates の実装は可能であることがわかった。