

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	PLC 命令列のハードウェア化と制御論理保護の一手法
------	----------------------------

産業用機器の制御論理は重要な知的財産であり、ブラックボックス化して保護する技術が求められている。本研究では、プログラマブルロジックコントローラ（PLC）の制御プログラムをField Programmable Gate Array（FPGA）上の制御回路に変換してハードウェア化するにあたり、難読化技術を適用して解析困難な制御回路を生成する方法を検討した。

難読化とは、プログラムや回路などの保護対象を、機能的に等価かつ構造や動作が複雑なものへと変換することで、その解析を阻害する技術である。本研究では、回路の出力を変えないという条件下で、PLC命令列からハードウェア記述（HDL）を生成する際に難読化を適用した。PLC命令列が条件分岐と処理を逐次的に実行する構造であることに着目し、**Opaque Predicates**と呼ばれる難読化手法を適用した。

Opaque Predicatesは、実行されない条件分岐や出力に影響しない条件分岐を追加することにより複雑化を実現する手法である。この手法では、分岐に用いる条件式の解析を困難にする必要があり、動的な有向グラフを用いてこうした条件式を生成する方法がCollbergらにより提案されている。ハードウェア記述化したPLC命令列に**Opaque Predicates**を適用する場合、PLC命令の実行条件となるif文の内部に新たなif-else文を追加し、その条件式を常に真（または偽）となるよう設定する。条件式を真に設定した場合、if-else文のif文側が常に実行されるため、if文側に本来の処理を記述し、else文側には任意の処理を記述する。常に真（あるいは偽）となる条件式には、Collbergの提案した手法（非連結な有向グラフ）を用いた。

提案した難読化適用方法の有効性を確認するため、2種類の小規模なPLCプログラムに対して難読化を適用した。プログラム1では極めて単純なPLC命令列に対し提案手法を適用し、追加された処理に対応するハードウェアが生成されることを、回路規模と動作周波数により確認する。プログラム2では実用的なPLC制御プログラムの一部に提案手法を適用し、難読化により追加された命令が回路の複雑さに与える影響について、回路規模とFan-out数の総和、回路規模あたりのFan-out数を用いて評価する。

プログラム1への難読化適用結果では、演算命令の追加に伴う回路規模の増大、動作周波数の低下が見られた。そのため本手法は、ハードウェア化したPLC命令列に適用可能である。プログラム2への難読化適用結果では、難読化により追加される命令のデスティネーションをもとの命令から変更した場合とそうでない場合において異なる傾向の結果が得られた。論理規模の増加量は前者が最大3.5%程度、後者は最大30%程度であった。Fan-out数の増加量は前者が最大1.5%程度、後者は最大20%程度であった。論理規模あたりのFan-out数はいずれの場合も難読化を適用しない場合を下回り、後者では最大5%程度低下した。論理規模、Fan-out数の平均値はいずれの場合も、難読化を適用しない場合を上回ったため、回路複雑化の効果が得られたものと考えられる。またデスティネーションの変更を含まない場合において回路規模あたりのFan-out数の減少幅が小さいことから、こうした命令を追加することにより、回路規模の増大を抑制しつつ難読化が実現できると考えられる。