令和 3 年 1 月 8 日

電気・電子情報工学専攻	学籍番号	M173266
申請者氏名	山田 翔太郎	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	ハードウェア難読化のための難読化指標の検討

ハードウェア（論理回路）上に実装された知的財産 (IP) の保護は重要な課題である．IP を保護する方法の一つに，ハードウェアやソフトウェアなどの機能を変えないまま内部構造を複雑化させて解析を困難にする技術である難読化が存在する．論理回路の難読化を直接行おうとすると，開発プラットフォームの相違や難読化によるタイミング特性の変化などの問題がある．そこで，ソフトウェア難読化と高位合成を組み合わせることにより難読化論理回路を生成する方法が松岡らによって提案された．高位合成は論理回路の設計手法の一つで，アルゴリズムレベルの記述から論理回路を生成する．先行研究では難読化によって回路のレイテンシ・論理規模が増大することのみ確認しており，実際に論理回路が複雑化してリバースエンジニアリングが困難となったかが検証されていない．高位合成や論理合成による最適化によって難読化がキャンセルされる可能性があるため，難読化論理回路が実際に難読化されているかどうかは検証が必要である．

そこで本研究では，論理回路の複雑度を定量化するために難読化指標を提案し，評価に用いる．LLVM ベースの高位合成ツール LegUp とソフトウェア難読化ツール Obfuscator-LLVM (OLLVM) を組み合わせることで，難読化ソフトウェアを高位合成することで難読化論理回路を生成した．

評価方法としては，ベンチマークプログラムを難読化・高位合成して論理回路を生成し難読化指標の測定を行う．高位合成前の LLVM IR (Intermediate Representation，中間言語) を対象にしたソフトウェア段階での評価と，高位合成後のネットリストを対象にしたハードウェア段階での評価を行った．実験には高位合成向けのベンチマークである CHStone を用いた．CHStone は C 言語で記述された 12 個の高位合成可能なプログラムからなる．OLLVM は偽の制御フロー (B)，制御フロー平坦化 (F)，命令置換 (S) の三種類の難読化手法を実装しており，それぞれを単独で適用した場合について評価を行った．

ソフトウェア段階での評価では，難読化された LLVM IR および高位合成の前処理として最適化などを経た LLVM IR を対象に難読化指標の測定を行った．3 種類の難読化手法のそれぞれで 8 種類の難読化指標を測定した．複雑度の上昇よりも回路規模の上昇が測定されてしまっていると考えられる指標が存在したため，それを除くと最大 (B) 111.5%，(F) 320.4%，(S) 102.8% の指標の増大が見られた．さらに，高位合成時の最適化によって減少する指標も確認され，これが難読化のキャンセルの原因の一つであると考えられる．

ハードウェア段階での評価では回路設計情報であるネットリストを対象に難読化指標の測定を行った．別の 3 種類の難読化指標を測定し，回路規模の上昇が測定されている可能性のあるケースを除外すると最大 (B) 3.61%，(F) 23.5%，(S) 4.15% の上昇が確認された．

難読化によって回路が複雑化していることを確認できたが，複雑度の変化と実際のリバースエンジニアリングの難易度の関係について評価することは今後の課題である．