

電気・電子情報工学専攻		学籍番号	M143276	指導教員氏名	市川 周一 藤枝 直輝
申請者氏名	松岡 佑海				

論 文 要 旨 (修士)

論文題目	LLVM と高位合成ツールによるハードウェア難読化の試験評価
------	--------------------------------

近年，ソフトウェアの著作権侵害が大きな問題となっている．この脅威からソフトウェアを保護するための保護技術の 1 つに難読化が存在する．難読化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が複雑になるように変換し，解析を阻害する技術である．また別の保護技術としてハードウェア化がある．ハードウェア化によりソフトウェアと比較して解析・盗用・改ざんが困難になると考えられる．近年注目されている高位合成を利用することにより，設計者は RTL より高い抽象度で設計可能となり，設計に必要な労力と時間を削減可能である．

本研究では Pascal ら (2015) がコンパイラ基盤である LLVM で実装した難読化ツール oLLVM を使用する．oLLVM は中間表現 (IR) で難読化を施すため，フロントエンドを変える事によって，多種多様な言語に難読化を施すことが可能である．oLLVM の出力は難読化した中間表現 (IR) であるため，さらにバックエンドによる変換が必要である．出力された LLVM IR を C 言語に変換する C バックエンドを使うことによって，難読化 C プログラムを生成する．難読化 C プログラムは高位合成ツールである Vivado HLS によってハードウェア化する．

評価は原ら (2009) が C ベースの高位合成 (HLS) 用に開発した CHStone で行う．CHStone は算術演算やメディア処理，セキュリティなどの様々なアプリケーション領域から選択された 12 のプログラムで構成されている．しかし，CHStone は Vivado HLS 用ではないため，いくつか問題が発生した．主な問題点は，Vivado HLS がポインタのサポートを制限していることである．本論文では，このサポート外の表現を解決する方法についても取り扱う．

ソフトウェア評価では実行時間とコードサイズを評価した．その結果，暗号アルゴリズム AES に制御フロー平坦化を施したものの (AES_F) は，実行時間が AES の 12.7 倍となり，BLOWFISH や SHA における実行時間比 (それぞれ 3.6 倍，6.7 倍) と比べて大きいことが分かった．各アプリケーションのコードサイズ比は 3 倍前後であった．この結果は AES が for 文と switch 文の両方を多用しているためと考えられる．ソースコードにおいても，for 文の使用数は AES，SHA，BLOWFISH の順になっている．これより，制御フロー平坦化が正しく動作していると考えられる．

偽の制御フローを施した AES (AES_B) と，BLOWFISH_B，SHA_B のコードサイズは 5.5 倍，7.8 倍，3.8 倍となり，実行時間は 3.7 倍，3.8 倍，4.4 倍となった．この結果より，BLOWFISH_B が最も実行時間に対するコードサイズの増加の少ないことが分かった．

ハードウェアの評価結果では，制御フロー平坦化を施すと，全てのプログラムで FF と LUT 使用量が上昇する事が分かった．また，偽の制御フローや命令置換を施した AES などの一部のアプリケーションではハードウェア使用量の減少も見られた．