平成30年度　卒業研究報告書概要

課程，学籍番号，氏名	課程: 電気・電子情報工学課程，学籍番号: B173266，氏名: 山田 翔太郎
工学分野名: 情報通信システム	指導教員名: 市川 周一，藤枝 直輝

題　　目: 和

oLLVMとLegUpを用いた難読化制御論理回路の試験評価

（英　Preliminary evaluation of logic circuit obfuscation with oLLVM and LegUp　）

Abstract

Obfuscation of logic circuits requires development of an obfuscation tool that is devoted to specific platforms and obfuscation methods. Matsuoka proposed to use oLLVM, a general-purpose software obfuscator, for logic circuit obfuscation by using high-level synthesis. In Matsuoka's method, LLVM IR obfuscated by oLLVM is converted to a C source code via CBE, and then Vivado HLS is used to generate the obfuscated hardware. On the other hand, LegUp is a LLVM-based high-level synthesis tool that can directly process IR generated by oLLVM, which could potentially solve the problems of Matsuoka's method. In this paper, Matsuoka's method is more accurately examined by logic synthesis and simulation of obfuscated circuits. LegUp is evaluated in the same way for the use in logic circuit obfuscation. It has shown that LegUp generates less efficient circuits than Vivado HLS, while LegUp alone can produce correctly working circuits for all combinations of programs and obfuscation methods that were evaluated.

概　　要

制御プログラムに含まれる知的財産の開発には多くのコストと時間が費やされており，その保護は重要な課題である．そこで，制御プログラムの論理回路化によって秘匿性の向上をはかる研究が行われてきた．論理回路を難読化することによって秘匿性をさらに高める方法も研究されてきたが，論理回路の難読化にはプラットフォーム・難読化手法に応じて専用のツール開発が必要であった．松岡はLLVMベースのソフトウェア難読化ツールoLLVMを用いてプログラムを難読化し，それを元に高位合成を行うという方法での論理回路難読化を提案した．この方法では，oLLVMが出力する難読化されたLLVM中間言語 (LLVM IR) をCバックエンド (CBE) を用いてC言語プログラムに変換し，高位合成ツールVivado HLSで高位合成を行う．しかし，CBEを通すという工程があるためにオーバーヘッドが存在する可能性がある．また処理の過程で難読化がキャンセルされ，論理回路に反映されないという問題があった．松岡の研究では作成した難読化論理回路の論理合成・論理シミュレーションを行っておらず，回路の正確なレイテンシやハードウェア使用量，また回路が正常に動作するかが未確認であった．一方で，LegUpと呼ばれるLLVMベースの高位合成ツールを用いると，難読化結果のLLVM IRから直接高位合成を行えるため，難読化のキャンセルやオーバーヘッドといった問題が解消されうる．

本研究ではまず，松岡の手法で生成した難読化論理回路の論理合成・論理シミュレーションを行った．その結果，Vivado HLSとCBEを用いる方法では一部のプログラムと難読化手法の組み合わせで作成した難読化論理回路が正常に動作しないという問題が判明した．また，oLLVMが実装する3種類の難読化手法のうち2種類で難読化がキャンセルされていると考えられる結果が得られた．

次に，LegUpを用いてoLLVMの出力するLLVM IRから直接高位合成を行う方法を評価した．その結果，CHStoneの12個のプログラム及びそれらに3種類の難読化を加えた場合の全てで，正常に動作する回路が生成できた．一方，高位合成結果の回路はVivado HLSと比較してレイテンシがCHStoneの全てのプログラムの平均で42.7%大きく，ハードウェア規模もLUT・FFのそれぞれで平均して41.6%，112%増大した．これはVivado HLS・LegUp間の最適化性能の差であると考えられる．また，難読化がキャンセルされるという問題もVivado HLSを用いる方法と同様に発生した．

正常に動作しない回路が生成されるという問題は解決したものの，高位合成ツール自体の性能差が大きく，また難読化がキャンセルされるという問題も解決していない．難読化のキャンセルについては，高位合成の過程が公開されているLegUpでは最適化・難読化パスの順番を調整するなどして改善できる可能性があるが，これは今後の課題とする．

発表する際の課程を記入　電気・電子情報工学　課程　　発表番号 69

（学籍が他課程所属の学生も発表する課程を記入すること）