2023 年 12 月 1 日

電気・電子情報工学専攻	学籍番号	M203256
申請者氏名	板東 伸彦	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	高位合成による Logic Locking 手法の実装と評価

近年，大規模集積回路の製造コストの上昇に伴って多くの企業がファブレス化しており，集積回路の製造を外部委託している．製造の外部委託により，リバースエンジニアリングによる IP（Intellectual Property）の盗用などが懸念されるようになった．このようなセキュリティ上の脅威から IP を保護するために，論理回路のネットリストを難読化する手法が提案されている．この手法の 1 つとして，回路に正しい鍵値が入力された場合にのみ，回路が正常に動作する手法（ロジック・ロッキング）がある．これらの手法の多くはハードウェア記述言語（HDL）を用いており，ネットリストレベルで組み込まれるものが多かった．近年では，C 言語など高級言語による動作レベルの記述から HDL 記述を自動的に生成する技術（高位合成技術）が提供されている．高位合成技術を利用することで，容易かつ高速にロジック・ロッキングを組み込むことが可能になり，より実用的な場面で使用可能になる．

武田（2020）は Yasin ら（2019）が提案した高位合成とロジック・ロッキングの 1 つである SFLL-HD を組み合わせた手法を参考に，高位合成用のベンチマークである CHStone に SFLL-HD を組み込んだ場合のシミュレーションと実装を行った．CHStone に用意されている動作テスト用の出力データを使用し，ロッキングによる出力の破損状態を調査した．出力の破損状態は間違った鍵値を使用した場合の出力と，正しい鍵値を使用した場合の出力を比べて，不一致となる比率により評価を行った．CHStone のアプリケーションの中から 3 種類のアプリケーションにロジック・ロッキングを組み込んだが，出力の不一致比率は期待値の最大値よりも約 4.2 倍大きくなる場合もあった．

武田の実験結果が期待値から外れた原因は，ロジック・ロッキングの対象が不適切であることだと考えた．そこで，CHStone アプリケーションにおいて，武田の手法とは異なる部分をロジック・ロッキングの対象としてシミュレーションを行い，武田の結果と比較した．武田は「一部の関数」をロッキングしたが，本研究では「回路全体」をロッキングした．また本研究では，シミュレーションする CHStone アプリケーションを武田の 3 種類から 8 種類に増やした．そして，アプリケーションごとに実装した際のリソース量を調査し，武田の結果と比較した．

シミュレーションの結果，提案手法は武田の手法よりも期待値に近づくことがわかった．計測値が 0 となるハミング距離を除いた全てのハミング距離において，本研究のシミュレーション結果の平均と期待値の誤差率は武田のシミュレーション結果の平均と期待値の誤差率よりも小さくなった．実装の結果，リソースオーバーヘッドはアプリケーションの規模によって違いがあることがわかった．小規模アプリケーションでは 10% 以上のオーバーヘッドが存在するが，中規模以上のアプリケーションでは約 3% 以下のオーバーヘッドしか存在しない．以上より，ロッキング技術を実用的に組み込むためには，一部の関数をロッキングするよりも回路全体をロッキングする方が有効であることがわかった．