令和 3 年 1 月 8 日

電気・電子情報工学専攻	学籍番号	M173237
申請者氏名	武田　真明	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	Logic Locking 手法の高位合成による試作と評価

近年，大規模集積回路の製造技術向上に伴い，回路設計を行うことを専門とするメーカ，設計をもとに製造を行うことを専門とするメーカなど細分化が行われている．設計を専門とするメーカは製造やテストを外部委託するため，設計技術が盗用されるなどの脅威に晒される可能性がある．そのため，設計技術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論理暗号化手法が提案されている．論理暗号化手法の一つとして正しい鍵が入力された場合に回路が正常動作するロジック・ロッキングが提案されている．しかし，これらの手法の多くはネットリストレベルで実装されており，より容易に実装するためには高位合成を利用してソースレベルで実装することが望まれる．

本研究では，Yasin (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 CHStone ベンチマークの DFSIN，JPEG，AES の 3 つのアプリケーションで適用し，シミュレーションと実装を行った．それぞれのアプリケーションから，戻り値があり，int 型の引数を持つ関数をロッキングの対象とした．シミュレーションでは不正な入力鍵が使用された際の出力の破損状況を調査した．出力の破損状況は正常に回路が動作した場合の出力に対して不正な値が出力された割合により評価を行った．入力データとして使用したデータは CHStone ベンチマークの動作確認用のテストベンチで使用されているものを使用した．鍵は 32 ビットの 5 つの組み合わせを用意し，ハミング距離は 0 から 32 まで変化させた．実装の際には Xilinx 社の HLS 用のソフトウェアである Vivado HLS 2020.1 を使用し，ロジック・ロッキングの適用前に対するリソースとレイテンシのオーバーヘッドを評価した．

シミュレーションの結果，DFSIN ではハミング距離が 14 のときに鍵ごとの出力の破損の差が最も大きく 59.4%，JPEG ではハミング距離 17 のとき 85.8%，AES ではハミング距離 13，14，15，18，19，20 のときに 100% であった．この結果から，SFLL-HD を使用した際には入力データの特性と鍵の組み合わせにより出力の破損の状況が大きく異なることが確認された．実装の結果，FF と LUT の使用数の増加が確認でき，DFSIN では FF が 0.826%，LUT が 3.57%，JPEG では FF が 6.05%，LUT が 20.0%，AES では FF が 11.2%，LUT が 21.8% のリソースのオーバーヘッドが確認された．なお，レイテンシは DFSIN では最大 2.48%，JPEG では 2.95%，AES では 13.9% のオーバーヘッドが確認された．リソースとレイテンシのオーバーヘッドはロッキングの対象とした関数が使用された箇所数が多い順に影響が大きいことが確認された．