論 文 内 容 の 要 旨

博士論文題目

Variation-Aware Hardware Trojan Detection through Power Side-channel Analysis

氏　　名　Fakir Sharif Hossain

(論文内容の要旨) 要

Hardware Trojans (HTs) are the malicious additions or modifications of circuit elements. The purpose of this dissertation is to improve the HT detection sensitivity in ICs using power side-channel analysis. This dissertation presents three detection techniques in power based side-channel analysis by increasing Trojan-to-circuit power consumption and reducing the variation effect in the detection threshold.

In the first method, a Golden IC based detection technique has been developed and an increased Trojan-to-circuit power consumption has been attained by a fine-grain scan based partitioning. Though Golden IC based detection suffers from both inter-die and intra-die variations, the sufficiently small partition size reduces the inter-die variation effect in the power consumption ratio. However, controlling the flip-flops in a segment requires a significant amount of extra hardware. The additional constraint of Golden IC free detection poses yet another challenge. These two issues have been addressed in the second proposed method by developing a novel clock tree driven circuit partitioning technique. The proposed equal-power self-referencing technique results in elimination of inter-die variation effects and increases detection sensitivity. To get a heightened detection sensitivity, the detection threshold has been reduced further in the third proposed method by addressing the intra-die systematic variation effect and by selecting a set of patterns that delivers a full toggling coverage.

Incorporating three proposed methods demonstrated that a realistic fine-grain circuit partitioning and an improved pattern set to increase HT activation chances can magnify Trojan detectability.

氏　名	Fakir Sharif Hossain

（論文審査結果の要旨）

平成29年12月20日に開催した公聴会の結果を参考に平成30年2月14日に本博士論文の審査を行った．以下のとおり，本博士論文は，申請者が独立した研究者として研究活動を続けていくための十分な素養を備えていることを示すものと認める．

本論文では，サイドチャネル情報である電力を解析し，以下を特徴とするハードウェアトロイ回路を検出する手法を提案している．

1. 被検査回路の一部を活性化させることで，ハードウェアトロイ回路以外で消費される電力を極力抑え，プロセスばらつきによる影響を抑えた検出手法を提案している．
2. 電力シミュレーションを用いて，同一回路の異なるセグメントから，ほぼ等しい電力を消費するテストパターン対を求めることで，ゴールデン参照回路を必要としない自己参照手法を提案し，ダイ間ばらつきの影響を受けない手法を提案している．
3. 回路上の隣接セグメントの電力を比較することで，ダイ内システマティックばらつきの影響を受けない手法を提案している．
4. クロックツリー上のクロックバッファをゲーティングすることにより，少ないハードウェアの追加で複数のFFを同時に制御する，ハードウェアオーバヘッドが小さくレイアウトへの影響が少ない手法を提案している．

半導体回路の設計・製造フローの多くのステージでのアウトソーシングが一般的となり，ハードウェアトロイ回路の挿入といったハードウェアセキュリティの脅威が現実的になり，それに対処する手法の開発が急務となっている．本論文は，半導体回路のセキュリティ向上に大きく貢献する実用的な内容であると評価できる．よって，本論文は，博士（工学）の学位論文として価値あるものと認める．