設計工程に侵入したハードウェアトロイの検出と耐ハードウェアトロイ設計技術の研究開発（141303001）

Research and Development on Hardware-Trojans Detection in IC Design Phase and Countermeasures against Hardware Trojans

研究代表者
戸川 望　早稲田大学
Nozomu Togawa　Waseda University

研究期間　平成 26 年度～平成 28 年度

概要

本研究開発では、集積回路の設計工程で侵入する不正回路（一般に、ハードウェアトロイと呼ばれる）に焦点を当て、まず設計工程のハードウェアトロイの性質を用いて、これらをいくつかのパタンとしてモデル化する。これらパタンに対して「スコア」を導入し、信号遷移回数ならびに最大スコア信号線数を観測することで、誤りのないハードウェアトロイ検出に成功した。続いて耐ハードウェアトロイ設計として、擬似トロイ信号線に「セキュアスキャン回路」を埋め込み、ハードウェアトロイと疑わしい信号線が回路中に存在しても、事前にこれを無効化する。実際に暗号回路などにセキュアスキャン回路を埋め込み、その効果を確認した。

１．まえがき

一般に、大規模集積回路（LSI）の設計・製造工程は、仕様記述から始まりいくつかの工程を経て最終製品として出荷される。一方、LSI の設計・製造工程は、設計や製造コストを削減するため積極的に外注を利用しているのが現状である。すなわち設計・製造プロセスにおいて、悪意ある設計･製造者が存在した場合､原理的に不正回路(ハードウェアトロイと呼ばれる）の侵入の危険性がある。そしてハードウェアトロイが侵入した LSI ならびにこれを用いたシステムは、一部もしくは全部の機能を無効・破壊される可能性や機密情報を漏洩する恐れがある。ハードウェアトロイにいかに対応するかは今後の電子産業において喫緊の課題と言える。

LSI の設計・製造工程は、主に設計工程と製造工程に分類される。後者の製造工程では 1 つのマスクパターンから多くの LSI チップを製造するのに対し、前者の設計工程ではただ一つの LSI 設計データを設計する。すなわち製造工程では多数の LSI チップの一部だけにハードウェアトロイを侵入した不正チップを作り込むことができるのに対し、設計工程ではただ一つの LSI 設計データにハードウェアトロイが侵入されると、これが不正設計データとなる。設計工程ではただ一つの LSI 設計データが不正かどうかを判断する必要があり、大きな問題点が存在する。

本研究開発では、LSI の設計工程におけるハードウェアトロイの不正侵入に焦点を当て、LSI 設計工程におけるハードウェアトロイ検出ならびに、耐ハードウェアトロイ設計技術に取り組んだ。

２．研究開発内容及び成果

2.1 設計工程ハードウェアトロイの検出

LSI 設計データの中に、ハードウェアトロイを構成する信号線（これをトロイネットと呼ぶ）をただ一つでも発見することができれば、これはすなわち当該の LSI 設計データがハードウェアトロイを含むことになる。またその逆に、LSI 設計データ中にトロイネットが一つも発見できなければ、これはすなわち当該の LSI 設計データが設計工程ハードウェアトロイを含まない正常設計データと言える。

そこで我々は、以下のアプローチをとることでこれを実現した:

(1) 設計データ中の全信号線集合の中から、トロイネット「らしい」ものを見つけ出す（弱識別ネット集合の抽出）。
(2) 弱識別ネット集合から、「確実に」トロイネットとなるものを見つけ出す（強識別ネット集合の抽出）。

そして、もし設計データ中に一つでも強識別ネットが発見されれば、その設計データは設計工程ハードウェアトロイが侵入したと考える。

2.1.1 弱識別ネット集合の検出

我々は、まず設計工程ハードウェアトロイの標準ベンチマーク Trust-HUB をもとにトロイネットの特徴的な性質を抽出した。その結果、全てのトロイネットは 9 個の性質に代表される。図 1 にその一部を示す（各ケースにおける太線がトロイネット「らしい」信号線であることを表す）。

設計データ中の各信号線において、図 1 の例に示すような 9 つの特徴のいずれか、あるいは、複数のものに該当するものを弱識別ネットと呼ぶ。弱識別ネットは、トロイネットである確率が高いと予想する。

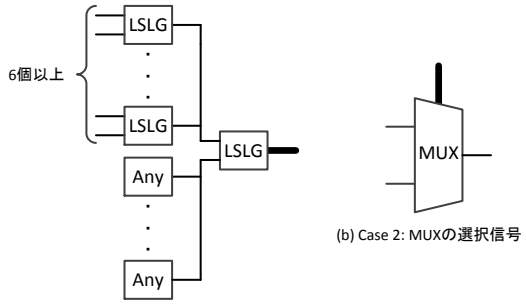

図 1：トロイネットの特徴の例

2.1.2 強識別ネット集合の検出

次に、弱識別ネットの中で「確実にトロイネットであるもの」を選別する。選別された信号線を強識別ネットと呼ぶ。強識別ネットは、以下の 3 条件（条件 1～条件 3）によって識別する。

《条件 1．スコア付け；スコア合計が 3 以上》 設計データ中の各信号線に対して、9 つのトロイネットの特徴それぞれにスコア

付けし、設計データ中の各信号線が 9 つの特徴にあてはまる毎にスコアを加算する。スコアが 3 点以上の信号線は強識別ネットとする。

《条件 2. 一定値を出力するクロックサイクル数；999,996 サイクル/1M サイクル以上》 弱識別ネットではあるが条件 1 を満足しない場合、まず「999,996 サイクル/1M サイクル」一定の値をとり続けるネットを抽出する。

《条件 3. 条件 2 を満足し最大スコアとなるネット数；5 以下》 次に条件 1 のスコア付けでスコア最大のネットを抽出したとき、最大スコアネットの数が 5 以下であり、かつ、その中で条件 2 を満足するものを強識別ネットとする。

そして設計データから一つでも強識別ネットを抽出した場合、これはトロイを構成するネットとし、その設計データはハードウェアトロイが侵入していると判断する。

2.1.3 Trust-HUB 全データ・ISCAS85 に関するハードウェアトロイ検出結果

提案技術を用いて、Trust-HUB 中の全ての論理レベル設計データならびに ISCAS85 ベンチマーク回路などの回路データを識別したところ、世界で初めて、すべてのデータに対して誤りなくハードウェアトロイの有無の識別に成功した。

2.2 耐設計工程ハードウェアトロイ技術の確立

設計データの中には、設計工程や製造工程にて完全にハードウェアトロイか非ハードウェアトロイかを判別することが原理的に不可能なものがある。このような信号線を擬似トロイネットと呼ぶ。擬似トロイネットに対して、チップ設計・チップ製造後も積極的にハードウェアトロイを検出するしくみを導入する。すると、万一、設計された回路データがハードウェアトロイを含む場合、チップ製造・チップ出荷後であってもハードウェアトロイの発現を回避することを可能とした付加価値を持ったチップ設計ができる。

そこで我々は、LSI 設計フローに「認証モード動作」・「通常モード動作」と呼ぶ動作モードを導入し、ハードウェアトロイを可視化、回路動作中に動的に擬似トロイネットを有効化・無効化するセキュアスキャン回路と、設計・製造後のチップに対してセキュアスキャン化による自己動的認証による安全なチップ設計・チップ動作を提案した。

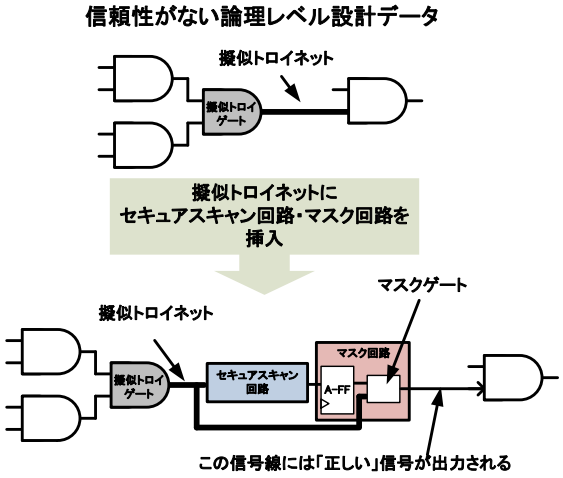

図 2：擬似トロイネットのセキュアスキャン化

図 2 に擬似トロイネットに挿入されたセキュアスキャン回路を示す。実際にハードウェアトロイが侵入した AES 共通鍵集積回路にセキュアスキャン回路を埋め込んだチップを試作した。鍵長ならびに平文・暗号文は AES 標準の 128 ビットとした。ハードウェアトロイ動作として、特定のパタンの平文が入力されたとき秘密鍵を暗号文として外部出力するものとした。

その結果、提案・構築したセキュアスキャン化による自己動的認証を行い、ハードウェアトロイが侵入していても、正常に AES 暗号回路動作することが実証された。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

本研究開発成果は、設計工程ハードウェアトロイ検出基準を見い出すと共に、擬似トロイネットに対するセキュアスキャン回路を開発する等、集積回路部品の信頼性に対して世界的に大きな成果を得ている。

これらの成果は、直接、IoT（Internet of Things；「もの」のインターネット）の高信頼化に大きく寄与するものと考えられ、今後、産業界と協力し、社会実装されることが期待できる。

４．むすび

本研究開発では、集積回路の設計工程で侵入するハードウェアトロイに焦点を当て、ハードウェアトロイの性質を用いて、これらを 9 つの特徴としてモデル化することで、ハードウェアトロイ検出に成功した。続いて耐ハードウェアトロイ設計として、擬似トロイ信号線に「セキュアスキャン回路」を埋め込みむことで、ハードウェアトロイと疑わしい信号線が存在してもこれを無効化した。実際に暗号回路などを通してその有効性を確認した。

【誌上発表リスト】

[1] R. Kitayama, T. Takenaka, M. Yanagisawa, and N. Togawa, "A Highly-Adaptable and Small-Sized In-Field Power Analyzer for Low-Power IoT Devices," IEICE Transactions on Fundamentals, vol. E99-A, no. 12, pp. 2348-2362（2016 年 12 月 1 日）

[2] M. Oya, N. Yamashita, T. Okamura, Y. Tsunoo, M.Yanagisawa, and N. Togawa, "Hardware-Trojans Rank: Quantitative Evaluation of Security Threats at Gate-Level Netlists by Pattern Matching," IEICE Transactions on Fundamentals, vol. E99-A, no. 12, pp. 2335-2347（2016 年 12 月 1 日）

[3] M. Oya, Y. Shi, N. Yamashita, T. Okamura, Y. Tsunoo, S. Goto, M. Yanagisawa, and N. Togawa, "A Hardware-Trojans Identifying Method Based on Trojan Net Scoring at Gate-Level Netlists," IEICE Transactions on Fundamentals, vol. E98-A, no. 12, pp. 2537-2546（2015 年 12 月 1 日）

【申請特許リスト】

[1] 戸川望、大屋優、ハードウェアトロイの検出方法、ハードウェアトロイの検出プログラム、およびハードウェアトロイの検出装置、日本、 2014 年 11 月 18 日

[2] 戸川望、大屋優、ハードウェアトロイ無効化方法およびハードウェアトロイ無効化装置、日本、2016 年 2 月 27 日

【受賞リスト】

[1] （受賞者）大屋優、（共著者）史又華、山下哲孝、岡村利彦、角尾幸保、後藤敏、柳澤政生、戸川望、（賞名）電気通信普及財団テレコムシステム技術学生賞、"A Hardware-Trojans Identifying Method Based on Trojan Net Scoring at Gate-Level Netlists," 2016 年 3 月 29 日

【本研究開発課題を掲載したホームページ】

http://www.togawa.cs.waseda.ac.jp/research/secu.html#ht