公益財団法人 セコム科学技術振興財団
研究成果報告書

研究課題名

高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発

Development of Trojan-free LSI system design and verification technology for highly secure and reliable information communication

研究期間

平成 30 年 10 月 ～ 令和 4 年 9 月

報告年月

令和 4 年 12 月

研究代表者
東北大学　電気通信研究所　教授
本間　尚文

Professor, Research Institute of Electrical Communication, Tohoku University
Naofumi Homma

概　要

本研究では，近年その脅威が指摘されているハードウェアトロイ（Hardware Trojan：HT）に対して，先端的かつ多様な HT をも検出・排除可能な系統的な LSI システムの設計・検出手法の確立を目指し，主要な基盤技術の研究開発を推進した．具体的には，LSI 製造を担うファブにおいて HT 混入の可能性は極めて低いという想定においても脅威となる（1）設計仕様から回路機能の基本設計を行うフロントエンド（Front-End: FE）設計時におけるソフトウェア IP コア（ハードウェア記述言語 HDL コードの形で提供されるサードパーティ製の機能ブロック）を介した HT 挿入，（2）HDL コードによる回路記述からレイアウトデータを設計するバックエンド(Back-End: BE)設計時におけるハードウェア IP コア(LSI 上にレイアウトされた形で提供されるファブの設計ライブラリやサードパーティ製の機能ブロック）を介した HT 挿入，(3) LSI 製造後のパッケージングおよびシステム実装時・実装後のプリント基板等への HT 挿入に対して，それぞれ設計段階で HT を検知するための基盤技術を開発した．

FE 設計時の HT 検知技術としては，回路仕様と回路記述（HDL コード）を変換する ZDD（Zero-suppressed Binary Decision Diagram）に基づく形式記述に基づく HT 検知手法を開発し，その有効性を国際標準暗号 AES（Advanced Encryption Standard）ハードウェアコアへの適用により実証した．同手法では，設計仕様および対象ハードウェア（HDL コードもしくは合成後のネットリスト）から得られる（連立）代数方程式を各々ZDD に基づく形式記述に変換し，変換後の記述の一意性と合流性から，その等価性を検証する．変数の変更や余分な機能の追加など機能改変を伴うハードウェアトロイ全てを検出可能であり，実際に実用的ハードウェアにおいても現実的な時間で検出できることを示した．

BE 設計時の HT 検知技術としては，ファウンドリの論理セルライブラリおよびサードパーティ製のハードウェア IP コアにより生成されたトランジスタレベルの物理レイアウト(GDS)に対して，設計データのシミュレーションによる製造前検証とウェハレベルテストによる製造後検証の統合により，BE 設計時の HT フリー性を電気的に保証する技術を開発した．まず，抽象度の異なる HDL と GDS における回路の物理特徴量をマルチテストシナリオの下でのシミュレーションにより相関付け，設計の改ざんに対する検知感度を獲得した．その上で，ウェハレベルテストによる測定データとの符合評価による製造後の検証を実現した．

システム実装時の HT 検知技術としては，HT が混入する可能性のある基板上の配線レイアウトおよび HT に利用される可能性のある素子配置を検出するシステム設計時の HT 挿入困難化技術を開発した．具体的には，システムレベルで挿入される HT をその機能で分類し，個々の HT を実現するための回路構成を明らかにした．続いて，その知見を元に HT を取り付けやすい基板およびペリフェラル（周辺素子）のレイアウトパターンを抽出し，LSI のレイアウトデータや入出力ピン配置等のシステム構成データから HT が実装される可能性のあるレイアウトおよび潜在的に HT として振る舞う可能性のある素子配置を検出し，その抑止手法について検討した．

本研究で開発した上記技術は，情報システムを設計・製造する過程において，HT の混入する可能性を設計の上流（論理設計）から下流（回路レイアウト）まで縦断して排除・抑止するものであり，本研究で開発した主要な技術を適切に組み合わせることにより HT によるインシデントを未然に防ぐ基盤となり得る．さらに本研究で開発した技術は，今後 AI を搭載した組込みシステムにおける HT による誤動作や停止・暴走を防ぐ基幹技術ともなり得るものであり，将来その重要性は益々高まると予想される．