2025 年度年次報告書

先端国際共同研究推進事業
【2024 年度採択　次世代のための ASPIRE　半導体分野】

【研究課題名】
LSI の真正性保証基盤によるトラスト社会の創出

研究代表者：
塩見 準（大阪大学　准教授）

主たる共同研究者：
新谷 道広（京都工芸繊維大学　准教授）
増田 豊（名古屋大学　准教授）

相手側研究代表者：
Alex Orailoglu（Professor, University of California, San Diego）

1. 研究進捗状況と成果

分散システム中に混入したハードウェアトロイの脅威に打ち勝ち、超スマート社会の持続的成長を実現するために、集積回路の真正性保証基盤の実現を目指す。ハードウェアトロイとは、サプライチェーンの中で、信頼できない存在により集積回路に挿入される悪意あるモジュールであり、分散システム中に混入したハードウェアトロイを検出し、その脅威を取り除くために、テーマ A～D に取り組んだ。

【テーマ A】真正性のモデル化、および真正性保証の高効率化ハードウェア技術

ハードウェアトロイに起因するスイッチング電力を増幅する電源機構を 2024 年度に提案した。この電源構造を利用し、スイッチングしていない状態のハードウェアトロイを検出する技術を Co-PI と開発した。真正性のモデル化の一環として、電磁的サイドチャネル情報量の電源電圧依存性のモデル化を行った。新原理コンピューティング技術である光 AI アクセラレータに対するレーザー故障注入攻撃の危険性と対策技術について、米国側 PI と国際共著発表を行った。日本側 PI が米国側 PI の研究室に約 2 ヶ月間滞在した。同時期に日本側 PI の指導学生 2 名が米国側 PI の研究室にそれぞれ約 1 ヶ月滞在した。

【テーマ B】真正性保証の容易化設計

攻撃側の検討として、2024 年度に提案した Cryo-HT の中間電位に起因するリーク電流抑制回路を検討し攻撃手法を洗練化させた。防御側では、米国側 PI らとの議論に基づき、AdaTrust を高度化する「テストパターン逐次改良戦略」を検討し、MT-fill と Random 戦略を段階的に組み合わせることで、不要なスイッチングを抑えつつトロイ由来の電力差を 2 倍以上拡大できることを確認した。さらに、180nm 極低温スタンダードセルを開発し、特殊環境下でのサイドチャネル解析基盤を確立した。また、日本側 PI との連携により、具体的には、シャドウ FF を活用した高速トグリング手法を検討しており、回路内部の信号遷移を意図的に活発化させることで、微小な HT による異常を顕在化させる技術の開発を進めている。

【テーマ C】ソフトウェアベースの低コスト LSI 真正性保証

ハードウェアトロイ回路の動的な消費電力を相対的に際立たせるテストパタン生成手法を洗練化した。自動テストパタン生成に基づく遷移故障テストと故障リスト分割を組み合わせる手法を提案した。また、遷移故障リストに対するテスト網羅性を維持しつつ、1 パタンあたりに同時検査される故障数を抑制するテストパタン生成法を検討した。さらに、分散 AI システム等への応用を見据え、近似コンピューティング技術など親和性の高い計算パラダイムに基づく LSI の設計検証についても並行して研究を進めた。

【テーマ D】（全 PI、Co-PI）実応用に資する真正性保証分散システム

テーマ A で述べた日本側 PI および指導学生 2 名の滞在期間に、日本側全 Co-PI も米国側 PI を訪問し、技術交流やテーマ D の議論を行った。テーマ D は国際頭脳循環に関わるため、国際頭脳循環を加速させる特別セッションやワークショップイベントをそれぞれ 1 件ずつ開催した。

2. 代表的な成果事例

1. K. Nishida, Y. Midoh, N. Miura, S. Kawakami, A. Orailoglu and J. Shiomi, "PrometheusFree: Concurrent Detection of Laser Fault Injection Attacks in Optical Neural Networks," 2026 31st Asia and South Pacific Design Automation Conference (ASP-DAC), 2026, pp. 1152-1159.

概要: 光 AI アクセラレータに対するレーザー故障注入攻撃の危険性を、光要素回路を用いて実測で示した。レーザー故障注入攻撃を再現するシミュレータを作成し、同攻撃の実行時検知技術を提案した。