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

2024 年度 年次報告書・公開版

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

日本側研究代表者 塩見 準 大阪大学 准教授

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

研究期間 2024 年 12 月 1 日～2028 年 3 月 31 日

1. 研究成果の概要

本研究では、分散システム中に混入したハードウェア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 (塩見 PI) 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

テーマ B (新谷 Co-PI) 真正性保証の容易化設計

テーマ C (増田 Co-PI) ソフトウェアベースの低コスト LSI 真正性保証

テーマ D (日本側 PI、日本側 Co-PI、米国側 PI (Alex Orailoglu 教授)) 実応用に資する真正性保証分散システム

① 研究構想にかかる成果

<実施したこと>

【テーマ A】LSI (Large Scale Integration、大規模集積回路) の真正性判定確率を解析モデルの構築に向けて、電磁的サイドチャネル情報、特に電源電圧依存性の測定と評価を行った。また、ハードウェアロイ (HT) 起因のサイドチャネル情報 (消費電力) を増幅する真正性保証の高効率化ハードウェア技術を 3 に示す[1]、[3]にて発表した。また、新奇デバイスによる新原理コンピューティング技術の将来的なエッジ環境への普及を見据えて、光コンピューティング技術を例にハードウェアセキュリティ技術の研究を米国側 PI と共同で行った。

【テーマ B】低温で動作する HT 回路を提案した。従来の HT は電気的狀態によって起動するが、提案する Cryo-HT はトランジスタの温度特性を利用する。具体的には、Cryo-HT は MOS 容量の放電時間を利用して、温度が下がると指数関数的に増加する放電時間をトリガとして起動する。シリコンによる概念実証に向け、180nm プロセスを用いて Cryo-HT を組み込んだ AES (Advanced Encryption Standard) 回路を設計、試作した。恒温槽を用いた測定により、Cryo-HT は室温では動作せず、低温で動作し、AES 回路の暗号鍵を抽出できることを確認した。さらに、サイドチャネル解析の高精度化に向けて低温時のトランジスタ電流のモデルを開発した。

【テーマ C】LSI の真正性保証に向けたソフトウェアベーステスト手法として、HT の動的な消費電力を強調するテストパターン生成手法を研究した。シミュレーション評価により、HT の Relative Power Difference (RPD) を増大させることを実験的に確認した。また、Compute-intensive なアプリケーションと親和性の高い計算パラダイムである近似コンピューティング (AC) 回路の設計技術を研究し、[5]にて発表した。

【テーマ D】ハードウェアセキュリティに関するワークショップに新谷 Co-PI が参加し、ハードウェアセキュリティに関するトップ研究者とネットワーキングを行った。分散システムの真正性保証技術について、日本国内での勉強体制を確立するため、分散システム・セキュリティの国内の著名な研究者数名と打ち合わせを行い、共同研究の可能性を探究した。

<得られた成果>

テーマ A～C について、国際会議で 2 件、国内学会およびワークショップで 5 件発表した。うち 2 件についてはそれぞれ 2025 年度に受賞が確定している。また、テーマ D について、分散システム・セキュリティの国内の著名な研究者数名とのネットワークを構築した。

② 国際ネットワーク構築・拡大／国際頭脳循環の促進に資する若手研究者の人材育成に関する成果

<実施したこと>

国際会議 ASP-DAC（2025年1月東京開催）でハードウェアセキュリティに関する特別セッション（審査あり）を企画し、日本側研究者（塩見 PI、新谷 Co-PI）、米国側 PI が研究成果の発表を行った。当該セッションにて、日本側全研究者（塩見 PI、新谷 Co-PI、増田 Co-PI）および米国側 PI が研究内容について意見交流を行った。塩見 PI の指導学生 1 名と塩見 PI 自身が米国側 PI の研究室に滞在し（2 人合わせて 26 日間の出張）、細粒度電源ドメイン分割技術の共同研究を行った。

<得られた成果>

日本側研究者と米国側 PI の共同国際学会セッションの開催、当該セッションにおける全 PI/Co-PI による意見交換会を開催した。指導学生 1 名と塩見 PI が米国側 PI の研究室に滞在し、テーマ A の共同研究を行った。

2. 研究実施体制

研究テーマ	中心となる研究者氏名	所属機関・部署・役職名
研究テーマA	塩見 準	大阪大学・大学院情報科学研究科・准教授
研究テーマB	新谷 道広	京都工芸繊維大学・電気電子工学系・准教授
研究テーマC	増田 豊	名古屋大学・大学院情報学研究科・准教授
研究テーマD	全PI/Co-PI Alex Orailoglu	(Alex Orailoglu の所属情報) University of California, San Diego・ Department of Computer Science and Engineering・Professor

3. 代表的な業績（原著論文、プレスリリース、表彰など）

- [1] Takahiro Ishikawa, Kose Yokooji, Yoshihiro Midoh, Noriyuki Miura, Michihiro Shintani, Jun Shiomi, "Hardware Trojan Detection by Fine-grained Power Domain Partitioning," 30th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 1257- 1263, Jan. 2025.
- [2] Ayano Takaya, Ryuichi Nakajima, Jun Shiomi, Michihiro Shintani, "Cryo-HT: Hardware Trojan Activated at Cryogenic Temperatures," 30th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 1264- 1269, Jan. 2025.
- [3] 石川貴大、御堂義博、三浦典之、新谷道広、塩見準「ハードウェアトロイ検出を可能にする細粒度電源ドメイン分割回路の低コスト化」信学技報、vol.124、no.400、VLD2024-127、pp.138-143、2025年3月 ※電子情報通信学会 VLD 研究会優秀技術報告賞の受賞確定
- [4] 高谷彩乃、中島隆一、塩見準、新谷道広「低温環境下におけるトランジスタ特性を用いたハードウェアトロイの開発」信学技報、vol.124、no.400、VLD2024-128、pp.144-149、2025年3月※電子情報通信学会 VLD 研究会優秀技術報告賞の受賞確定
- [5] 山口 明生、増田 豊、石原 亨「反復計算回数と演算ビット幅の削減に基づくクリティカルパス・アイソレーション回路の低消費エネルギー化」第 252 回 ARC・第 208 回 SLDM・第 68 回 EMB 合同研究発表会（ETNET2025）、no.46、pp.1-8、2025年3月