2022 年度
創発的研究支援事業 年次報告書

研究担当者	原 祐子
研究機関名	東京工業大学
所属部署名	工学院
役職名	准教授
研究課題名	IoT エッジ向け組込みハードウェア/ソフトウェアのセキュア設計
研究実施期間	2022 年 4 月 1 日～2023 年 3 月 31 日

研究成果の概要

IoT/組込みデバイス台数の劇的な増加に伴い、IoT セキュリティ強化の重要性が高まっている。近年、特にネットワークセキュリティの問題が取り上げられているが、データ通信前にデバイスから情報が漏洩することを抑止するために暗号処理の搭載が必要になる。しかし、計算・メモリ資源が限られたデバイスには従来の暗号アルゴリズムは実装困難なため、軽量暗号の研究開発や標準化の動きが活発に行われている。一方、暗号処理する計算機システムの電力等のサイドチャネルを狙った攻撃（サイドチャネル攻撃）によって数学的に堅牢な暗号も破られうるため、サイドチャネル攻撃耐性（耐タンパー性）を持つ IoT/組込みデバイス設計技術の確立は喫緊の課題である。

本研究では、耐タンパー性を持つ暗号システムのハードウェア・ソフトウェア協調設計手法の確立に取り組む。既存の耐タンパー設計はハードウェアあるいはソフトウェアのどちらかであったのに対して、本研究で初めて両者を活用した協調設計手法を確立することで、耐タンパー設計によるオーバーヘッド（回路面積あるいは処理遅延）のトレードオフを探索することが可能になる。

今年度は、ハードウェア・ソフトウェア協調設計で活用する技術の一つである高位合成に着目し、高位合成で耐タンパー設計を行う手法を確立した。高位合成はソフトウェア記述を入力としてハードウェア設計を行う上流設計技術で様々なアプリケーションのアクセラレータ設計に活用されてきたが、セキュリティを考慮しておらず、高位合成ツールが行う従来の最適化がサイドチャネル漏洩を引き起こしていた。本研究はセキュリティを考慮していない高位合成ツールを利用しつつ、漏洩を抑える設計手法を確立するとともに、耐タンパー設計による回路面積・処理遅延のオーバーヘッド、サイドチャネル漏洩を引き起こす最適化を明らかにした。