創発的研究支援事業
終了報告書

研究担当者	原 祐子
研究機関名	東京工業大学
所属部署名	工学院情報通信系
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～2024 年 3 月 31 日

研究成果の概要

本研究期間中は、IoT 機器への電力サイドチャネル攻撃を想定し、以下の 2 つの研究課題について取り組んだ。

1. 高位合成を用いたアクセラレータのセキュア設計

C 記述による高位合成を用いたセキュアなアクセラレータ設計を行った。具体的には、サイドチャネル攻撃への対策手法であるマスキングと高位合成のスケジューリング最適化（演算の並列化、チェイニング）を併用する方法を提案した。演算の並列化はマスキング理論と親和性が高く、既存の最適化手法を活用することができるが、一方でチェイニングはマスキング理論上で禁止されている最適化を行う可能性が高く併用は難しいことを明らかにした。これにより、セキュリティを考慮していない高位合成ツールで、セキュアなアクセラレータ設計を行う体系的手法を確立した。本研究成果は、FPGA 関連の一流国際会議（International Symposium on Field-Programmable Gate Arrays）、および、一流国際論文誌（ACM Transactions on Embedded Computing Systems）に採択された。

2. ハードウェア/ソフトウェアのマスキング協調設計

暗号アルゴリズムにマスキングを適用する際のハードウェア・ソフトウェアの協調マスキング手法を開発した。プロセッサで暗号アルゴリズムを処理する場合、ソフトウェアマスキングを行っていても演算（命令）間で共有するプロセッサ中のリソースが情報漏洩源となることが報告されていた。この漏洩を防ぐためには、より高次元のマスキングを適用する必要があり、レイテンシのオーバヘッドが非常に大きいことが問題であった。本研究では、ソフトウェアマスキングは攻撃者に応じた最低次元のマスキングを適用しつつ、プロセッサのリソース共有による漏洩は、省電力化のための従来のゲーティング技術を応用することで対策するという協調設計手法を提案した。ゲーティング技術自体は汎用的であるため、様々なプロセッサに適用可能である。情報漏洩を防ぎつつ、既存手法に比べて省面積かつ低レイテンシで暗号アルゴリズムを処理可能であることを示した。本研究成果は、一流国際論文誌（IEEE Internet of Things Journal）に採択された。