論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	A Power Side-channel Secure Embedded Processor for Lightweight IoT Applications
著者(和文)	YANGMingyu
Author(English)	Mingyu Yang
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第12707号, 授与年月日:2024年3月26日, 学位の種別:課程博士, 審査員:原 祐子,尾形 わかは,髙橋 篤司,本村 真人,佐々木 広,LI YANG
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第12707号, Conferred date:2024/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		Yang Mingyu	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	原 祐子	准教授	審査員	佐々木 広	准教授
	審査員	尾形 わかは	教授		李 陽 （電気通信大学 大学院情報理工学 研究科）	准教授
		髙橋 篤司	教授			
		本村 真人	教授			

論文審査の要旨（2000字程度）

本論文は，A Power Side-channel Secure Embedded Processor for Lightweight IoT Applications（軽量 IoT アプリケーションに向けた電力サイドチャネルセキュリティを有する組込みプロセッサ）と題し，英文6章から構成されている．

第一章 Introduction（緒言）では，IoT技術の発展に伴い増加している組込みデバイス，特に組込みプロセッサの技術的課題について述べている．特に注目されているアプリケーションとしてeHealth に着目し，そのようなアプリケーションでは処理時にかかる消費電力・エネルギーの効率化の他，データプライバシやセキュリティの要求が高まっていると述べている．さらに，暗号システムを搭載したデバイスでは，消費電力などのサイドチャネルから情報漏洩が起こりえる危険性について指摘している．これらの背景を踏まえ，本研究では低消費電力，かつ，電力サイドチャネル攻撃耐性を持つ組込みプロセッサを新たに提案・設計すると説明している．組込みプロセッサを定義する命令セットの検討から始め，電力サイドチャネルを防ぐためのソフトウェア開発手法，および，プロセッサの設計手法を提案し，軽量暗号およびeHealthアプリケーションへの展開可能性を実証することが本論文の目的であると述べている．

第二章 Background（背景）では，既存の組込みプロセッサとそのサイドチャネルセキュリティについて解説している．

第三章 The Small and Secure Processor（SSP）（小型かつセキュアなプロセッサ（SSP））では，提案プロセッサであるSSPの命令セットの詳細と，その妥当性について解説している．さらに，電力サイドチャネル攻撃耐性を強化するためのアーキテクチャ設計手法について解説している．

第四章 Protection against Power Side-Channel Attacks（電力サイドチャネル攻撃に対する保護）では，第三章で提案したプロセッサSSP上で軽量暗号を含める数種のアプリケーションを処理し，回路面積，処理性能（クロック周波数），消費電力・エネルギーを評価し，既存の組込みプロセッサに対するSSPの優位性を示している．さらに，電力サイドチャネル攻撃耐性を強化した既存プロセッサとSSPをFPGA上に実装した場合の潜在的な電力サイドチャネル漏洩を比較評価した結果，SSPには潜在的な漏洩がないことからSSPの優位性を示している．また，既存プロセッサで電力サイドチャネル漏洩が起きた要因についても知見を述べている．

第五章 Implementation of eHealth Applications（eHealthアプリケーションの実装）では，第四章で有用性を実証したSSPを，eHealthアプリケーションへ適用した場合のケーススタディについて示している．限られたメモリ容量でeHealth等の実用的なアプリケーションを処理するために，小容量メモリ指向のソフトウェア最適化手法について提案している．その手法によって実装したeHealthアプリケーションのソフトウェアをSSP上で処理した場合，リアルタイムで生体情報の異常を検出可能であることを実証している．

第六章 Conclusions（結言）では，本論文で得られた結果をまとめ，残された課題を述べている．

以上を要するに，本論文は，消費電力・エネルギーのみならず，データプライバシやセキュリティの要求が厳しいIoTデバイス向けの組込みプロセッサの実現に向け，命令セットの定義・アーキテクチャ設計手法，および，ソフトウェアの開発手法について新たに提案し，実用的な暗号システムおよびeHealthアプリケーションに対してその有用性を定量的に示していることから，学術的および工学的貢献は大きい．よって，審査員は本論文が博士（工学）の学位論文として十分に価値があるものと認める．