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)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	情報通信 情報通信	系 コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of	（ 工学 ）
学生氏名： Student's Name	Yang Mingyu		審査員主査： Chief Examiner	原 祐子	

要旨（英文 800 語程度）
Thesis Summary (approx.800 English Words)

The development of the Internet of Things (IoT) has brought about a transformative shift in daily life, creating a ubiquitous network of interconnected devices with profound impacts across various domains, particularly in healthcare through eHealth systems. This expansion facilitates real-time data processing and enhances medical care by leveraging vast amounts of biomedical data. However, the rapid integration of IoT, especially in eHealth, raises significant challenges in data privacy, security, and the need for secure hardware platforms.

A critical vulnerability in IoT security is the threat posed by power side-channel attacks. These attacks, capable of extracting secret information based on power consumption, are a significant risk in IoT devices that handle sensitive data. Such attacks exploit the correlation between power consumption and the secret information being processed by the device, allowing an attacker to extract sensitive information. This vulnerability is particularly concerning given the widespread use of IoT devices in handling personal and sensitive data, ranging from financial information to eHealth data. The inherent limitations of IoT devices, such as constrained power, memory, and the need for energy efficiency, further complicate the implementation of effective countermeasures. Traditional countermeasures, which are often resource-intensive, are not feasible for IoT devices due to these constraints.

Addressing these challenges, this research proposes a novel embedded processor optimized for lightweight IoT applications, emphasizing power efficiency, circuit area, and security. This processor features a unique Instruction Set Architecture (ISA) designed to minimize circuit area and power consumption while maintaining processing efficiency. This is crucial for IoT applications where resources are constrained, such as in wearable devices, sensor networks, and smart homes. The proposed processor is a significant advancement in the field of IoT, as it addresses the dual requirements of low power consumption and robust security, which are often at odds in conventional designs. Furthermore, the processor design significantly mitigates risks associated with power side-channel attacks. A hardware/software cooperative approach is adopted to optimize system performance and security. On the software side, hardware-aware optimizations are conducted to ensure secure and efficient operation with the underlying hardware. On the hardware side, a bottom-up methodology defines a minimal ISA and architectural structure, embedding efficiency and security as core considerations.

Experiments demonstrate the effectiveness of the proposed processor design in real-world scenarios. The experimental results in terms of side-channel security validate the processor's robustness in safeguarding secret information against power side-channel attacks. Furthermore, experiments in eHealth applications demonstrate the processor's capability to adeptly manage lightweight IoT applications while operating under stringent resource and power constraints. This dual achievement of operational efficiency and enhanced side-channel security, even in environments with limited energy resources, marks a notable advancement in the field of IoT.

In summary, the proposed embedded processor not only provides the ability to process lightweight IoT applications with low power consumption and minimal resource usage but also offers robust defense against power side-channel attacks, safeguarding sensitive information in resource-constrained environments. This research contributes to the development of a secure IoT ecosystem, achieving comprehensive security with the constraints of IoT devices and paving the way for advancements in IoT applications. The processor's innovative design is poised to revolutionize the way IoT devices are developed, focusing on energy efficiency and security as primary design criteria. This approach is expected to have far-reaching implications, not only in the realm of IoT eHealth but also in other fields where data security and power efficiency are of paramount importance. Future research can explore the integration of this processor in a wider range of applications, potentially leading

to more secure, efficient, and versatile IoT solutions. The principles established in this study can also guide the development of next-generation IoT devices that are capable of handling increasingly complex tasks while ensuring data privacy and security in an ever-connected world.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。

Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。

Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).