システムセキュリティ研究室

SDGs達成に向けた取り組み

研究テーマ・キーワード Research Themes・Keywords

安全なコンピュータの作り方を
研究テーマに情報セキュリティの研究分野を広く扱う

We broadly cover the field of information security with the research theme of developing secure computers

- 暗号処理システム Cryptographic Processing System
- システムアーキテクチャ Systems Architecture
- サイドチャネル攻撃対策 Countermeasure of Side Channel Attacks
- 近似計算 Approximate Computing

担当教員 Subject Teacher
請園 智玲 UKEZONO Tomoaki

PROFILE

職 位 Position: 准教授 Associate Professor
学 位 Degree: 博士(情報科学) Ph.D. in information science
担当講義科目 Charge of Subjects: ネットワークセキュリティ など Network Security etc
e-mail: tukezo@fuk.kindai.ac.jp

FOR MORE

UKEZONO Tomoaki

研究概要 Research Outline

放射電磁波や消費電力などからコンピュータ内部の秘密情報を漏洩させる攻撃があります。本研究室はこのような情報漏洩攻撃を防止する設計手法の研究をしています。

There are attacks that exploit electromagnetic radiation, power consumption, and other side channels to leak confidential information from within computers. Our laboratory researches on design methods to prevent such information leakage attacks.

進行中の研究内容 Research Contents in Progress

1. コンピュータの消費電力波形を利用した情報漏洩攻撃に対して、そのサイドチャネル攻撃を防御するオペレーティングシステム（OS）を開発し、情報漏洩攻撃に対する安全性を向上させる研究をしています。

   I am researching to develop an operating system (OS) that defends against information leakage attacks using the power consumption waveforms of computers, aiming to improve security against such side-channel attacks.

2. AESと呼ばれるインターネット標準暗号のサイドチャネル脆弱性を打ち消す回路構成法を研究しています。サイドチャネルから漏れる暗号鍵のヒントを隠す回路内部のデータの流れを制御する機構を提案しています。

   I am researching a circuit design to counter the side-channel vulnerabilities of the internet standard encryption called AES. I am proposing a mechanism to control the data flow inside the circuit in order to hide clues about the encryption key that may leak through side channels.

最近の研究実績 Recent Research Results

〈著書／Books〉

- 佐藤寿倫, Tongxin Yang, 請園智玲, "センサフュージョン技術の開発と応用事例", 株式会社 技術情報協会(単行本), 第6章 "センシング、機械学習を支える半導体デバイスの開発と応用", 第1節 , "近似計算の採用による画像処理の低消費電力化", pp.239--245, 2019年1月.

〈論文／Published Papers〉

- Ryoma Katsube, Shinichi Nishizawa, and Tomoaki Ukezono, "An EDA Based Side-Channel Attack Flamework for Netlists," Proc. of 2025 IEEE Region 3 Conferencex, 6-pages, Mar. 2025.
- Soma Kato, Yui Koyanagi and Tomoaki Ukezono, "An OS support for Tamper-resistant Software Execution Using Empty Interruptions," Proc. of 20th International Conference on Information Systems Security, Springer LNCS Vol. 15416, pp.25-41, 18-pages, DOI: 10.1007/978-3-031-80020-7_2, Dec. 2024.
- Yui Koyanagi and Tomoaki Ukezono, "Random Clock Gating for Side-Channel Protection," Proc. of 2024 IEEE Asia Pacific Conference on Circuits and Systems, pp.697-701, 5-pages, DOI: 10.1109/APCCAS62602.2024.10808212, Nov. 2024.
- Ryoma Katsube, Taiki Nagatomo, and Tomoaki Ukezono, "Flattening Power Waveforms by Hamming Distance Converter for Side-Channel Attacks," Proc. of 2024 IEEE Asia Pacific Conference on Circuits and Systems, DOI: 10.1109/APCCAS62602.2024.10808349, pp.231-235, 5-pages, Nov. 2024.