研究スタッフ

教　授：　本間　尚文

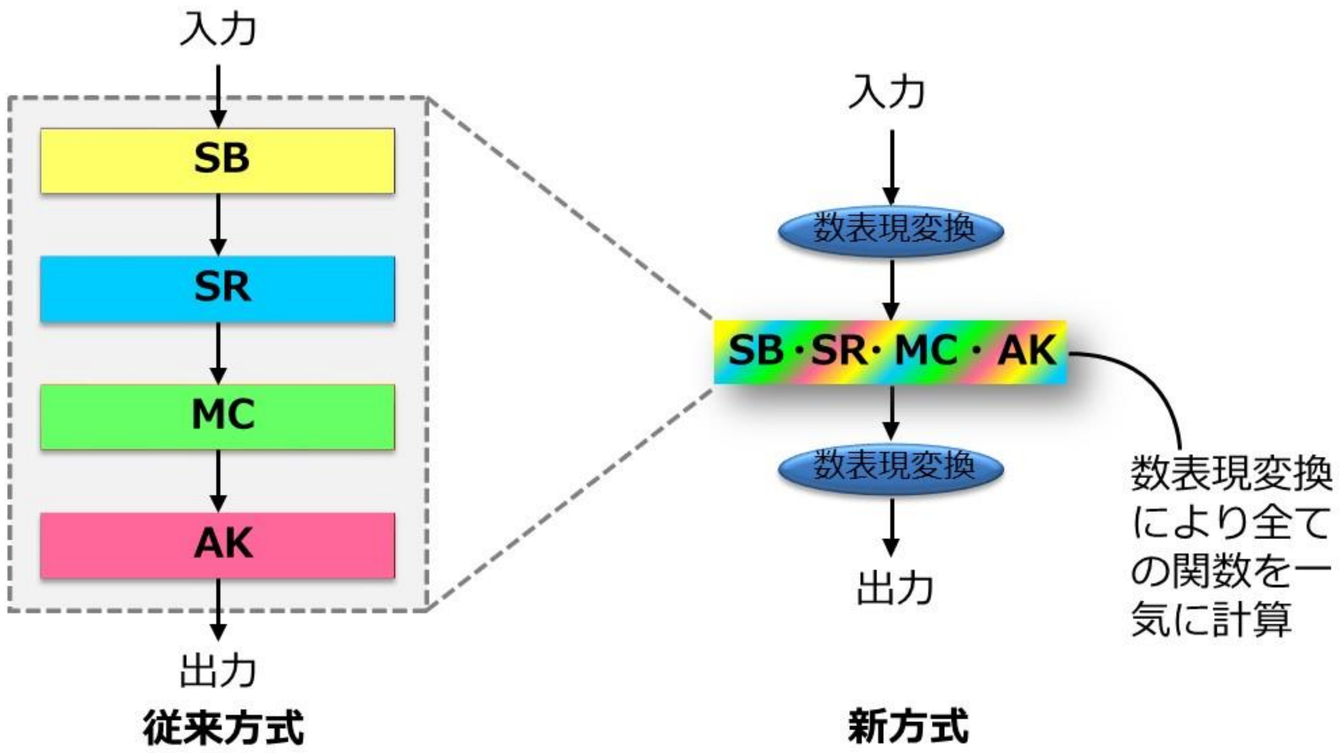
研究目的

本研究室では，暗号技術を中心とした次世代情報セキュリティ技術に関する研究に取り組んでいる．特にIoTやCPSといった次世代情報通信技術を誰もが安心して利用するための基盤となるハードウェアセキュリティ技術を暗号コンピューティングの理論からそのシステム実装技術にいたるまで，縦断的に探求している．

主な研究テーマ

1. 高機能・軽量・耐タンパー性セキュリティHWの設計

本研究では，現在の情報セキュリティの基盤技術である暗号をLSIシステムで実装するためのHWアルゴリズムを開拓している．特に，新たな暗号機能（グループ署名や秘密計算）を実現する高機能暗号や軽量暗号を対象として，そのハードウェアアルゴリズムを開発している．また，並行して，各種の攻撃に耐性を有する暗号ハードウェアアルゴリズムなどの開発にも取り組んでいる．

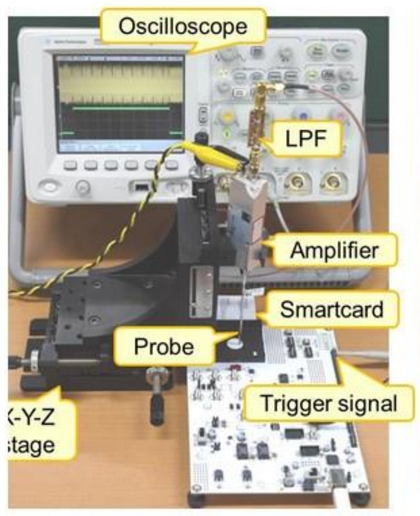


省エネルギーAES暗号ハードウェアのために新たに開発したハードウェアアルゴリズム（ガロア体の数表現変換により小型・高速な演算を実現）

2.組込みシステムのセキュリティ設計・解析技術

本研究では，ネットワークに接続する多様な組込みシステムに対する系統的なセキュリティ設計・解析技術の確立を目指している．特に，現在最も現実的かつ強力な攻撃とされているサイドチャネル攻撃（副次的な漏洩物理量の観測および副次的な故障誘発による攻撃）に対して耐性をもつ組込みシステムの設計・評価プラットフォーム開発を進めている．

これまでに開発した設計・評価プラットフォーム

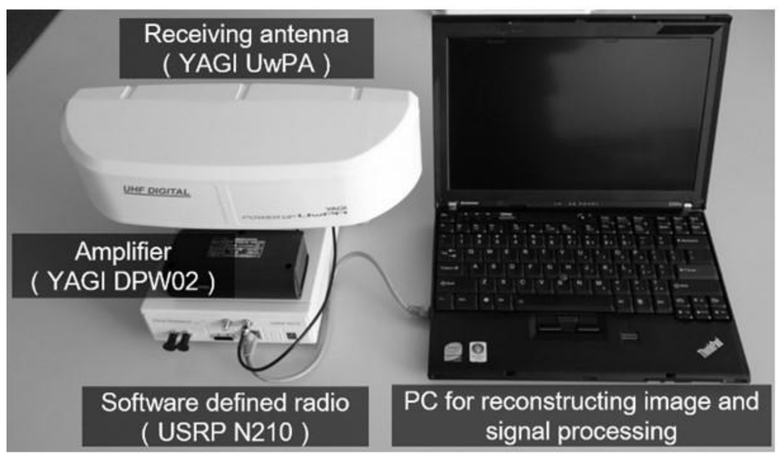


開発したプラットフォームを用いた評価システムの構築例

開発したプラットフォームの採用機関・企業・大学（欧米を中心にNISTをはじめとする各国の政府系機関でも利用されている）

3.電磁情報セキュリティの理論と応用

本研究では，放射電磁波による情報漏えいや一時的な故障誘発といった電磁波を介した情報セキュリティの問題に対して，そのメカニズムの解明を進めるとともに，電磁的な安全性解析・評価技術の研究開発に取り組んでいる．特に，タブレットやスマートフォンからの放射電磁波による「電磁的画像盗視」のメカニズム解明とその効果的な対策技術の開発を進めている．



産学連携を希望するテーマ例

- セキュリティハードウェアアルゴリズムの研究
- IoTシステムセキュリティの理論・実装技術の研究
- 次世代デバイスのセキュア実装技術の研究
- 電磁波を介する情報セキュリティの研究
- 組込みAIシステムのセキュリティの研究