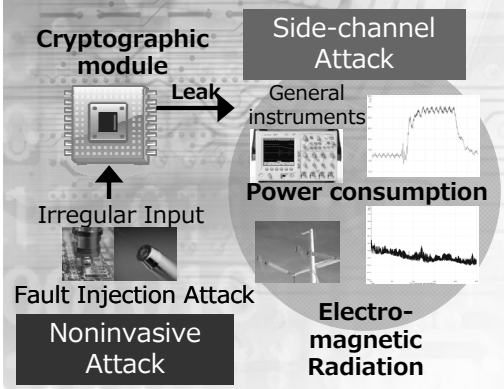
ICカードの実装安全性標準評価ボードSASEBO-W
- サイドチャネル解析のデモンストレーション -

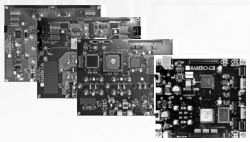
産業技術総合研究所　情報セキュリティ研究センター
片下敏宏　堀洋平　佐藤証

研究の背景と目的



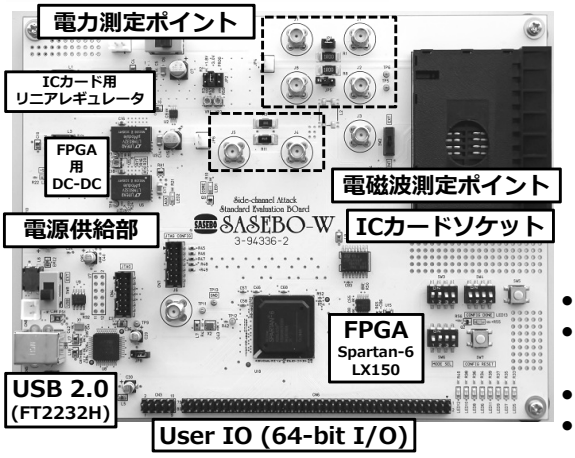
　標準化されている暗号アルゴリズムは理論的な安全性が十分検証されていますが，実装時の物理的な安全性は別の検証が必要となります．
　特に，暗号を実装したモジュールの消費電力や電磁波などの物理量を解析して内部の秘密情報を盗み出す「**サイドチャネル攻撃**」は大きな脅威であり，その対策手法の開発や安全性評価手法の標準化が急務となっています．
　サイドチャネル攻撃標準評価ボード**SASEBO** (Side-channel Attack Standard Evaluation BOard)は，これら研究や標準活動の促進を目的に開発されました．

サイドチャネル攻撃標準評価ボード



　異なるテクノロジのデバイスを用いた**４種の標準評価ボード**を開発しています．暗号をデバイスに搭載して実験できるよう，全てのISO/IEC標準ブロック暗号とRSA暗号回路を開発しており，これらの仕様，回路のコードをWebサイトで公開しています．

ICカードの実装安全性評価ボードSASEBO-W

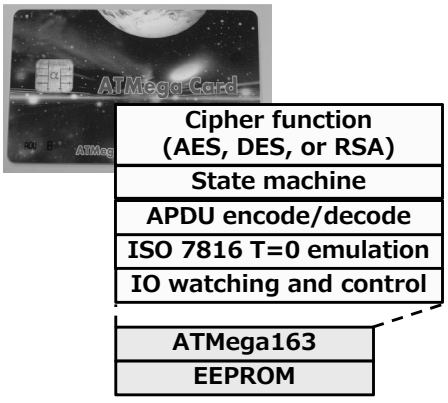


http://staff.aist.go.jp/akashi.satoh/SASEBO/ja/

SASEBO-W

　サイドチャネル攻撃評価対象の主要製品である**ICカードをターゲットとする新評価ボード**SASEBO-Wを開発し，評価試験・実験環境を構築しています．従来のカードリーダでは困難であった，**入出力信号の波形観測や，精密なトリガ調整による実験が可能**です．

- ICカードの電力や電磁波の測定が可能
- 1.3~5.9V可変のICカード電源
  信号レベルはカード電源へ自動的に調整
- **ICカードの全信号，電源はFPGAで制御**
- 最新のFPGA Spartan-6 LX150 により，**ICカード模擬や下位互換を実現**
- **USB2.0による電源供給**
  高速インタフェース
- 設計資料などをWebサイトで公開



暗号ICカード

　セキュリティ機能のない一般利用向けMPU ATMega 163カード上にICカードOSと暗号ソフトウェアを実装しており，**ICカードを用いたサイドチャネル攻撃実験**を行うことが可能です．

- ISO 7816-3 のT=0 プロトコルに対応
- 3種の暗号ソフトウェアを実装
  - AES (2種類の実装方式)
  - DES (T-DESに対応)
  - RSA (2種類の計算方式，2種類の実装方式)

お問い合わせ先

(独)産業技術総合研究所 情報セキュリティ研究センター ハードウェアセキュリティ研究チーム
チーム長　佐藤 証　akashi.satoh@aist.go.jp

SASEBO-Wの開発はJST戦略的国際科学技術協力推進事業（共同研究型）「日本－フランス共同研究」組込みシステムにおける暗号プロセッサの物理攻撃に対する安全性評価（SPACES）の一環として実施されたものである．