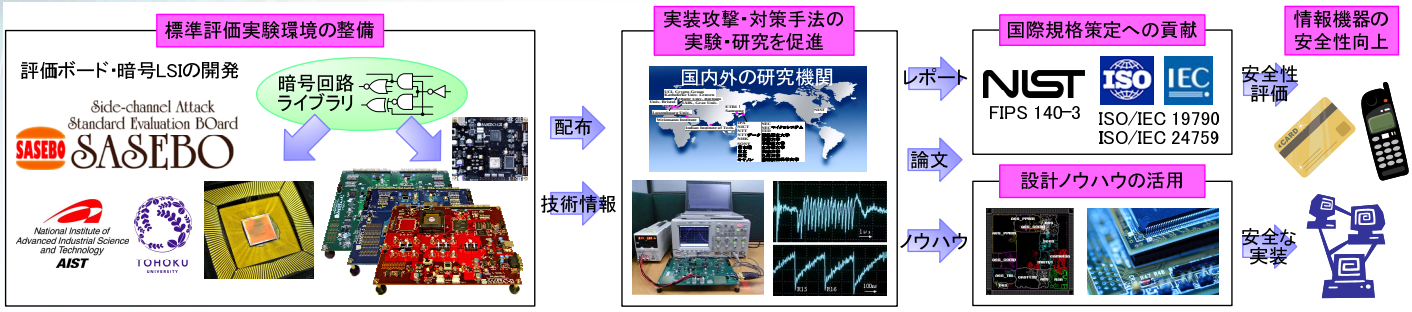
暗号モジュールの安全な実装を目指して
－ サイドチャネル攻撃の標準評価プラットフォームの構築 －

産業技術総合研究所　情報セキュリティ研究センター

研究の背景と目的

デジタル情報機器の急速な普及とともに，データ保護のための暗号技術の利用が進んでいます．暗号アルゴリズムの安全性が理論的に十分検証されていますが，実装の不備により情報が漏洩する恐れのあることが知られています．特に，暗号アルゴリズム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」が注目されており，その対策手法の開発や安全性評価指針の確立が急務となっています．

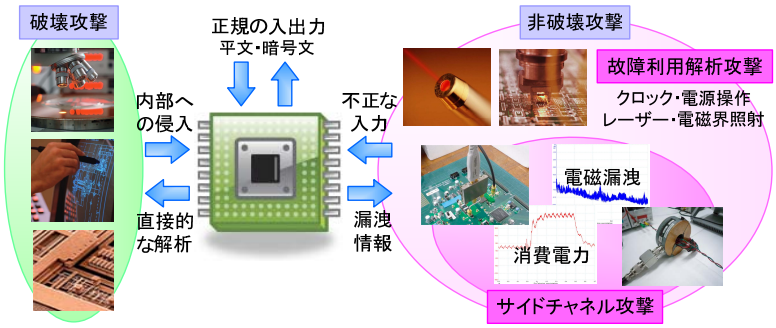
産業技術総合研究所と東北大学は，サイドチャネル攻撃の標準評価環境を構築することで国際規格策定を促進させることを目的に，標準評価ボードSASEBO(Side-channel Attack Standard Evaluation BOard)と専用暗号LSIを開発しました．SASEBOは国内外の研究機関へ配布されており，サイドチャネル攻撃研究の促進に大きく貢献しています．また，研究活動を通じて得られた知識や技術を積極的に公開しており，情報機器の安全性向上に取り組んでいます．



サイドチャネル攻撃とは？

サイドチャネル攻撃は，暗号モジュールの正規のチャネルを通じた暗号文・平文の入出力ではなく，消費電力や電磁波などの“サイドチャネル”に漏洩している物量から内部動作情報を解析することで，モジュール内の秘密情報を非破壊的に盗み出す非破壊攻撃の一種です．

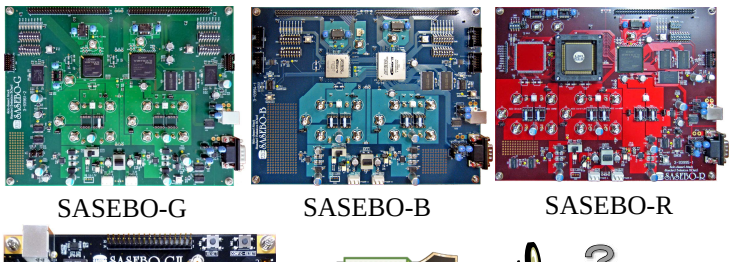
オシロスコープやパソコンなど容易に入手可能な機器で実行可能であり，攻撃の痕跡も残さないことから，その脅威が注目されています．



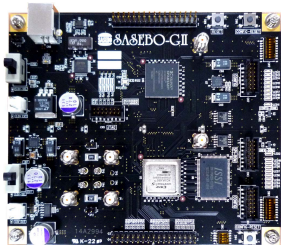
サイドチャネル攻撃標準評価ボード SASEBO (Side-channel Attack Standard Evaluation BOard)

異なる回路アーキテクチャによる評価実験を可能とするため，SASEBO-G(Xilinx版)，SASEBO-B(ALTERA版)，SASEBO-R(ASIC版)の3種類のボードを開発し標準評価ボートとして配布を行っています．SASEBO-R用の暗号LSIには，全てのISO/IEC国際標準ブロック暗号とRSA暗号が実装されています．本ボードの仕様書，ソースコード，制御プログラムはWebで公開されています．
(http://www.rcis.aist.go.jp/special/SASEBO/)

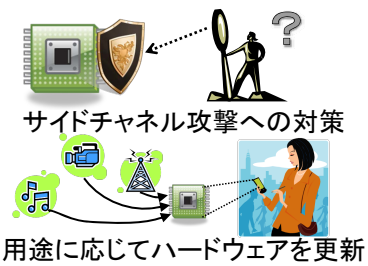
サイドチャネル攻撃の対策を組み込んだ暗号回路の評価を可能とするため，大規模ロジックを搭載可能なFPGA Virtex-5を搭載したSASEBO-GIIを開発しており，教育用ボードとして販売しています．本ボードは給電や制御をUSBインターフェースに集約してユーザビリティが向上されているほか，ハードウェアを動的に再構成する機能も搭載しています．



SASEBO-G　SASEBO-B　SASEBO-R



SASEBO-GII



お問い合わせ先

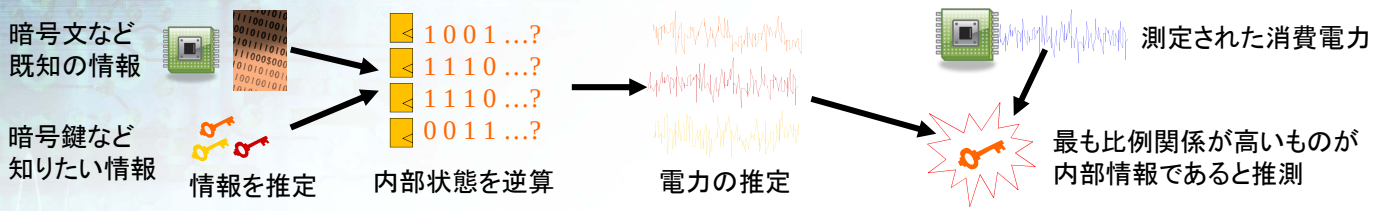
(独)産業技術総合研究所 情報セキュリティ研究センター ハードウェアセキュリティ研究チーム
チーム長　佐藤 証　akashi.satoh@aist.go.jp

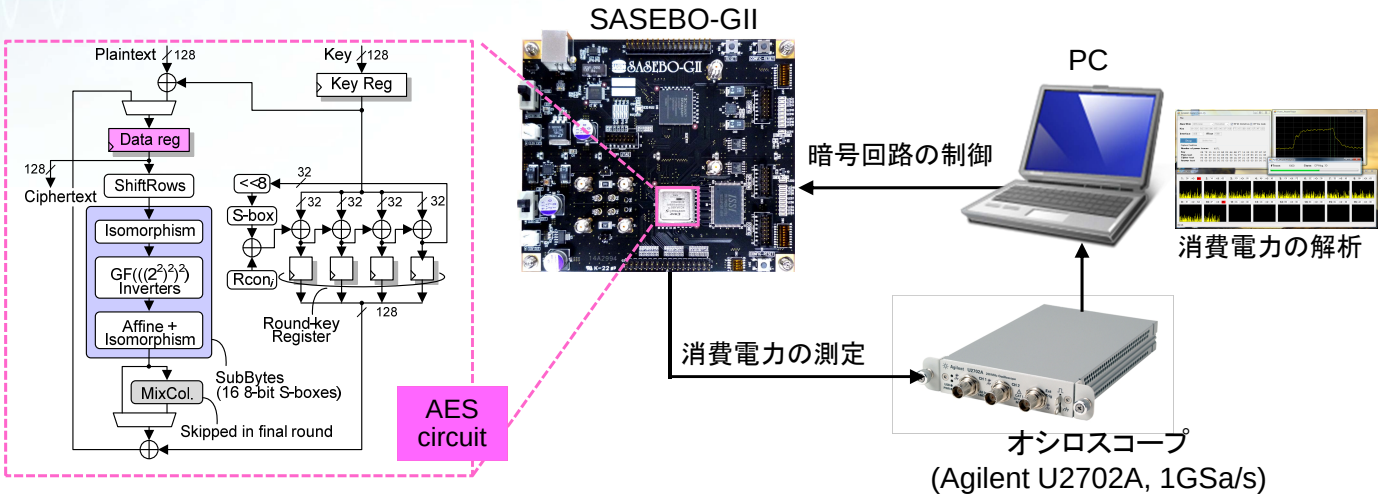
本研究は，経済産業省委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の一環として行われました．

サイドチャネル攻撃のデモンストレーション

SASEBO-GIIのFPGAにAES暗号回路を実装し，回路の消費電力をUSB接続のオシロスコープにより測定します．そして，測定された電力をCPA (Correlation Power Analysis)手法により解析し，回路内部の128-bitの暗号鍵を導出します．

CPAは回路の内部状態の変化が消費電力と比例すると仮定することで，消費電力から内部状態を推測します





デモンストレーションの画面