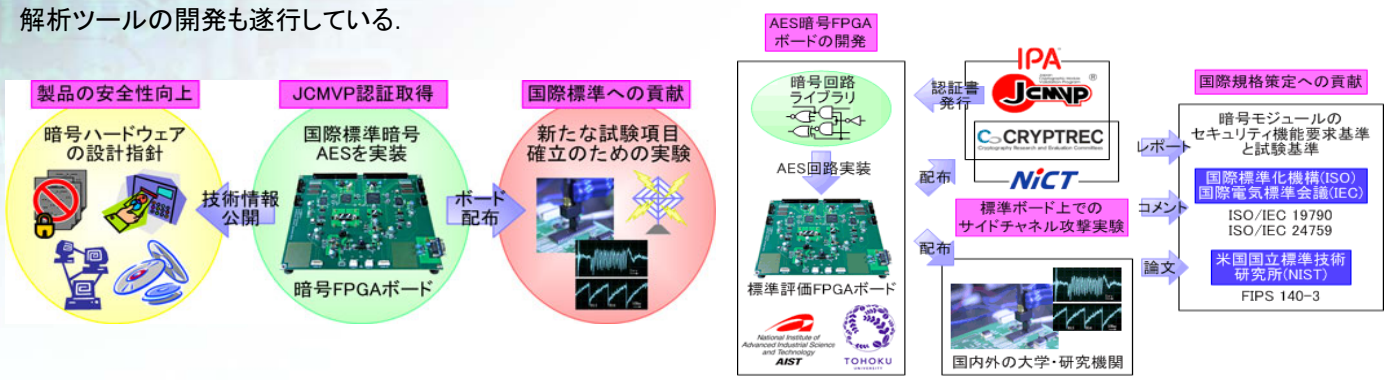
サイドチャネル攻撃標準評価ボードによる電力解析実験

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

研究の背景と目的

安全性が十分に検証された暗号アルゴリズムを利用した製品でも，実装の不備により機密情報が漏洩する恐れがある．そこで，暗号を実装したモジュールが満たすべき要件を定め，これを公的な第三者機関により評価する制度JCMVPが我が国で実施されている．近年では，暗号モジュールの動作中の電力波形などから内部情報を暴露する「サイドチャネル攻撃」が登場しており，その対策法の開発や新たな試験評価指針の確立が急務となっている．

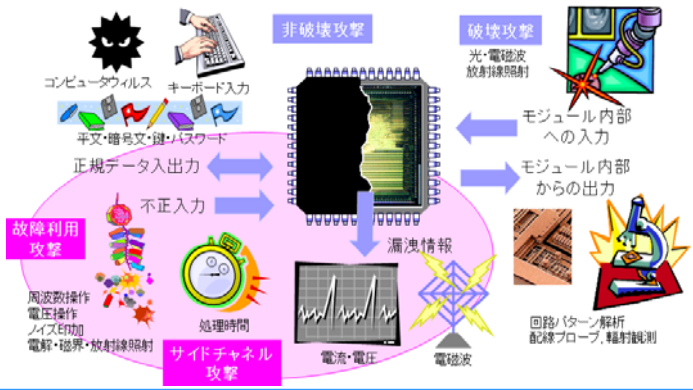
このような背景から我々は標準評価環境の構築を目的として，評価標準ボードや暗号ハードウェアマクロおよびLSIを開発し，国内外の研究機関へ配布している．サイドチャネル攻撃の効果は実験装置にも大きく依存することから，標準評価環境の配布により評価基準策定の促進することが期待されている。このほか，標準評価環境において評価手法の研究や解析ツールの開発も遂行している．



サイドチャネル攻撃とは？

サイドチャネル攻撃とは、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，処理時間などサイドチャネルから漏洩している内部動作情報を悪用してモジュール内の情報を非破壊的に暴露する方法である．モジュール内部を直接観測する破壊攻撃では高価な装置が不要であることから，その対策と評価手法の確立が急務となっている．

サイドチャネル攻撃の対策として内部処理のランダム化などの手法が提案されており，実験結果なども報告がなされているが，各々の研究機関が独自の実験環境を用いていたため第三者による追試や評価が難しいという問題があった．



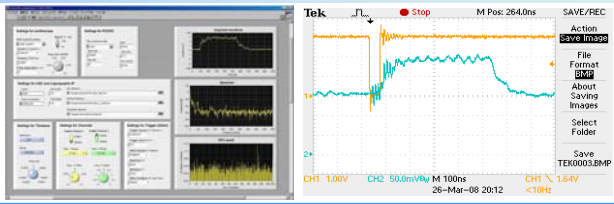
サイドチャネル攻撃標準評価ボード（SASEBO: Side-channel Attack Standard Evaluation Board）

標準評価実験環境の構築のため，回路を再構成可能なFPGAのボード2種と，全てのISO/IEC国際標準ブロック暗号を実装したLSIのボードを開発し，国内外の大学や研究機関に配布を行っている．

国際標準暗号AESを実装したFPGAボードは，暗号ハードウェアモジュールとして初のJCMVP認証を取得しており，それらの技術情報はWeb（http://www.rcis.aist.go.jp/special/SASEBO/）で公開している．

デモンストレーション

サイドチャネル攻撃への対策を施していないAES暗号回路をFPGAボード上に実装し，暗号処理中の電力波形をPCからの制御により自動的に取得する計測環境のデモンストレーションを行う．実際のサイドチャネル攻撃では，取得した数千パターンの波形を統計解析し暗号化に用いた秘密鍵の導出を行う．



お問い合わせ先

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，経済産業省の委託事業「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ている．