

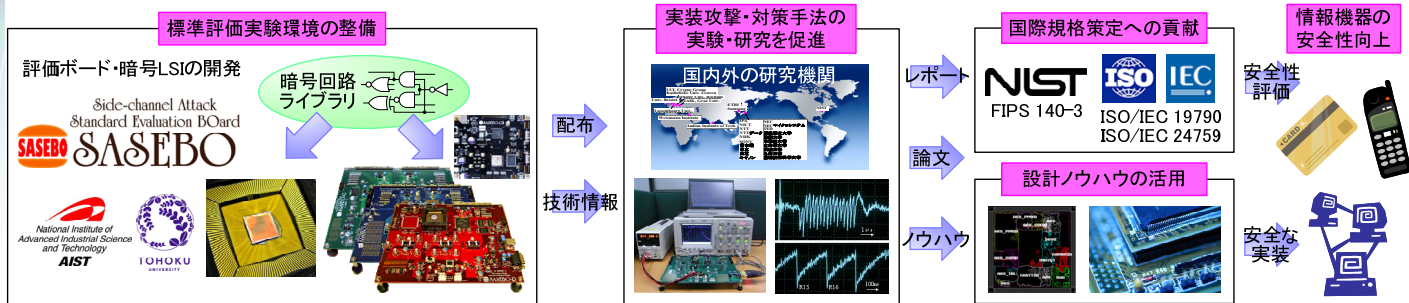
# 暗号モジュールからの漏えい情報を利用するサイドチャネル攻撃 － 標準評価プラットフォームによるリアルタイム解析実験 －

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。製品に実装される標準暗号はアルゴリズムの安全性が十分に検証されていますが、実装の不備により情報が漏洩することも珍しくありません。また近年、暗号モジュールの消費電力などから内部情報を盗み出す“サイドチャネル攻撃”が登場し、その対策手法の開発と安全性評価指針の確立が急務となっています。しかしながら、これまで、各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りました。

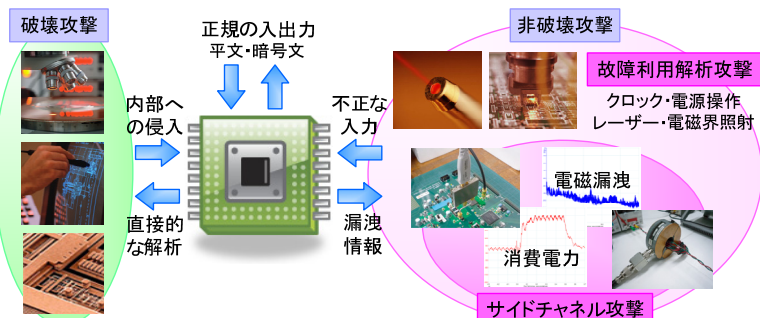
(独)産業技術総合研究所と東北大学は、サイドチャネル攻撃の標準評価環境を構築し国際規格策定に貢献することを目的に、標準評価ボードSASEBOと専用暗号LSIを開発しました。SASEBOは国内外の研究機関へ配布され、サイドチャネル攻撃研究の推進に大きく貢献しています。また、公的試験機関での利用を目的とした解析ツールの開発も行っています。これらの研究活動を通じて得られた知識や技術を積極的に公開し、情報機器の安全性向上に取り組んでいます。



## 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、そして処理時間などの“サイドチャネル”に漏洩している内部動作情報を解析し、モジュール内の機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、攻撃の痕跡も残さないことから、その脅威は現実のものとなりつつあります。

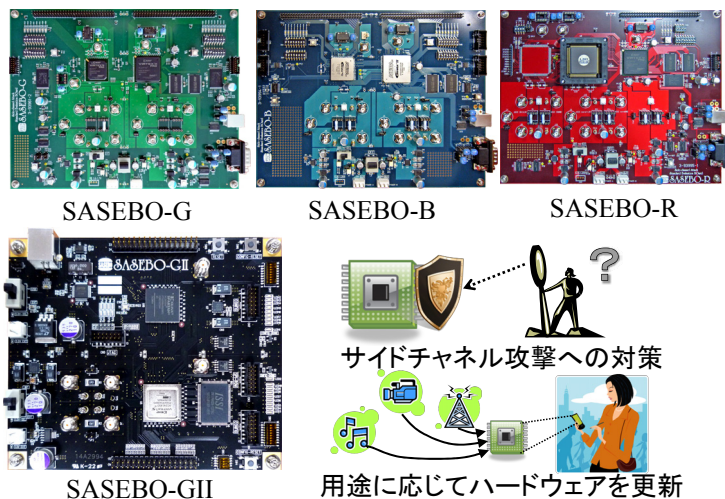


## サイドチャネル攻撃標準評価ボード SASEBO (Side-channel Attack Standard Evaluation BOard)

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試験装置としての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だけでなく、ハードウェアセキュリティシステムとしての安全性検証を可能とするため、大規模ロジックが搭載可能な最新の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の予定です。給電や制御を全てUSBインターフェースに集約してユーザビリティの向上を図ると同時に、ハードウェアを動的に部分再構成する機能も搭載しています。



## お問い合わせ先

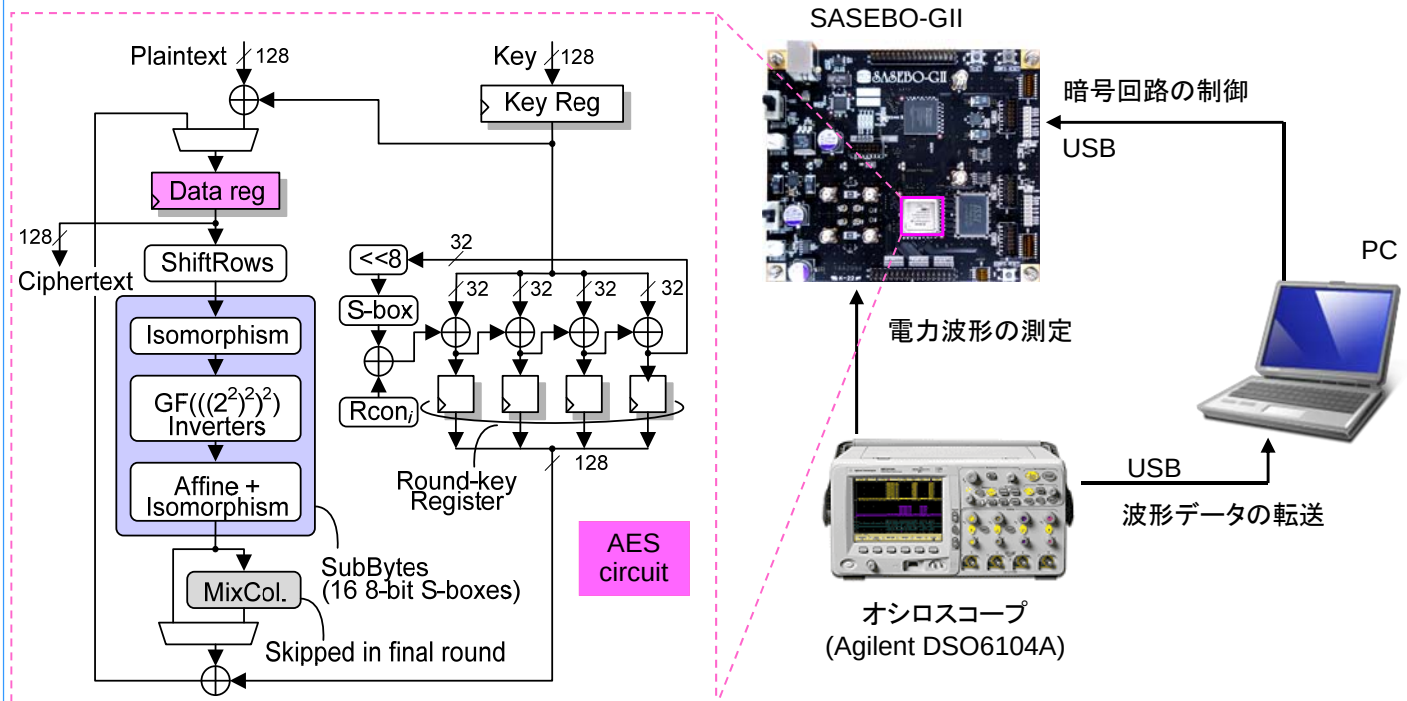
(独)産業技術総合研究所 情報セキュリティ研究センター ハードウェアセキュリティ研究チーム  
チーム長 佐藤 証 akashi.satoh@aist.go.jp

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ています。

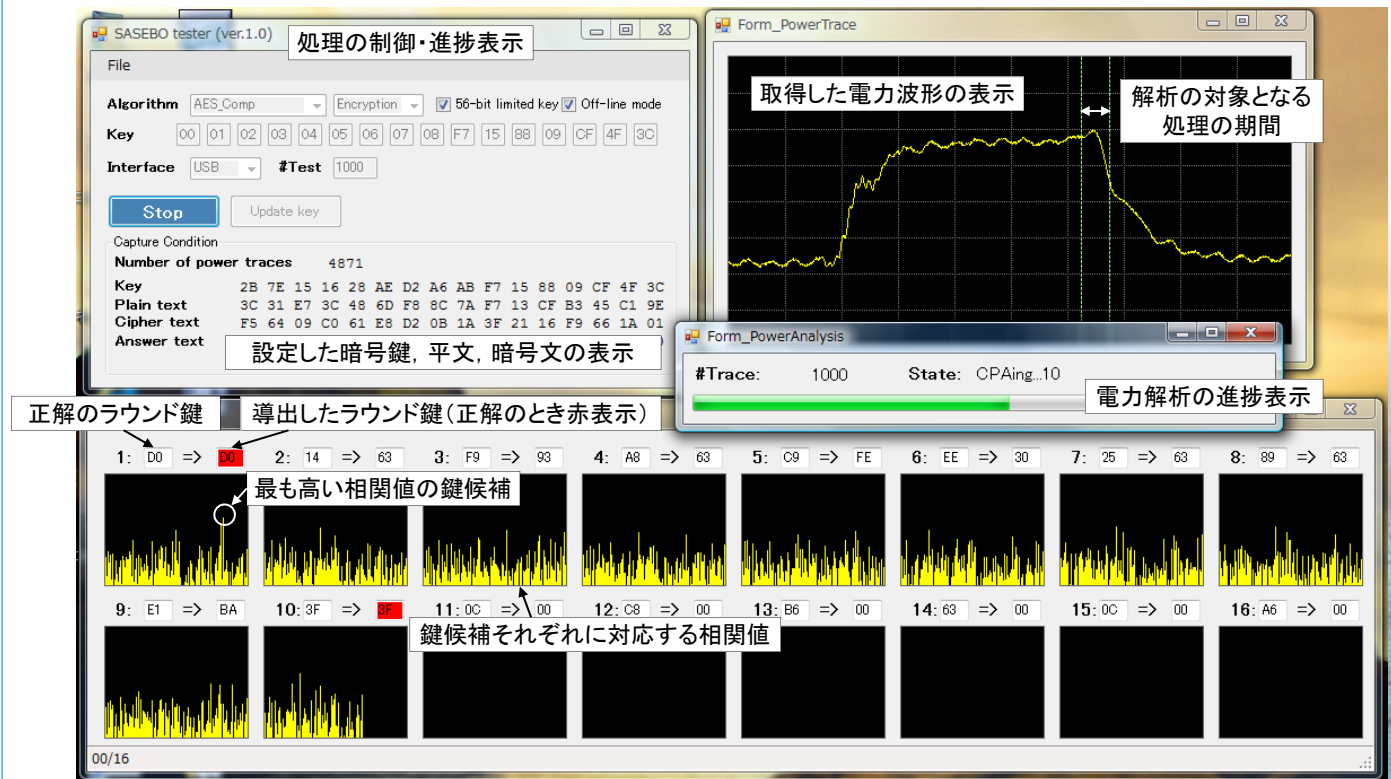
## デモンストレーションの詳細

SASEBO-GII, USB接続のオシロスコープ, パーソナルコンピュータで構成された環境で, 電力解析攻撃の1つである CPA (Correlation Power Analysis) によりAESの128bit秘密鍵を導出します。

- CPAではAES回路の内部データ(Data reg)のハミング距離が消費電力に比例するモデルを仮定します
- AESでは9ラウンドから最終10ラウンドの処理で32bit関数のMixcolumnsが省略されるため, 128bit鍵を16分割した8bitの部分鍵を独立に導出することができます
- $2^8=256$ 通りの部分鍵候補から消費電力モデルに最もマッチしたものを秘密鍵として推定します
- 精度の高い解析には電力モデルの対象でない回路が発生するノイズ成分を除去する必要があるため, 数千~数十万の電力波形を用いた統計処理を行います



## デモンストレーションの画面



## デモンストレーションソフトウェアの開発環境

Microsoft Visual Studio 2008, National Instruments Measurement Studio 8.6, FTDI D2XX driver, C#言語