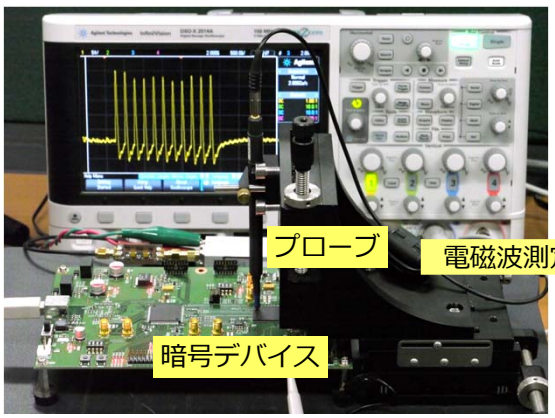
National Institute of Advanced Industrial Science and Technology
AIST

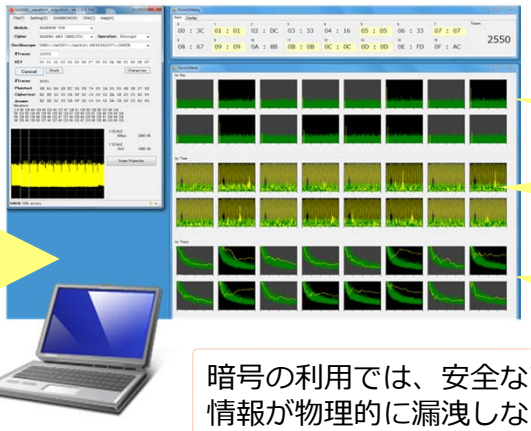
わずか数分で暗号が破れてしまう！？
- サイドチャネル攻撃の対策と安全性評価環境の構築 -

理論的な解読は
現実的な時間で不可能

消費電力・電磁波への漏えい情報を解析する手法
対策法の開発と安全性評価手法の標準化が急務

デモンストレーション



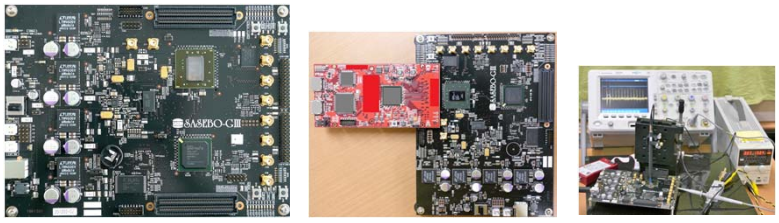


解析ソフトウェア

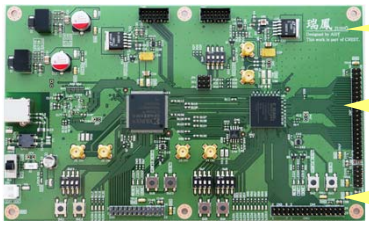
- 微小な変動を統計処理
- LSIから漏洩している電磁波変動の様子
- 無対策の暗号LSIの電力解析はわずか２～３分

暗号の利用では、安全なアルゴリズムとともに、
情報が物理的に漏洩しない安全な実装が必要

サイドチャネル攻撃標準評価環境の構築

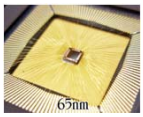


サイドチャネル評価ボード SASEBO-GIII
(Side-channel Attack Standard Evaluation Board)



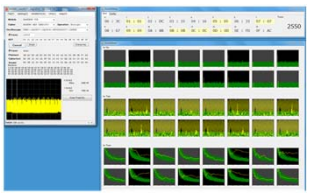
- 消費電力や電磁波の測定が容易
- 入門キットや新しい解析手法のテスト環境として最適
- ボードの製造・販売のライセンスをしています

サイドチャネル評価のトレーニング環境 ZUIHO
(お問い合わせは sasebo_info-ml@aist.go.jp まで)



e-shuttle
2x2 mm^2
23 cores
対策済LSI

暗号LSI評価ボード



解析・評価ソフトウェア

サイドチャネル攻撃への安全性を評価できる
サイドチャネル攻撃標準評価環境を開発

消費電力が小さい最新の 28 nm FPGAデバイスにおいても、暗号回路の鍵が解析可能

FMCドータボードに対応しており、HDMI、USB、イーサネットなどに暗号回路を実装した組み込みシステム全体で安全性を評価できる

暗号回路やボードの設計情報，解析ツール，評価実験レポート等をWebサイトで公開

Evaluation Environment for Side-channel Attacks
Side-channel Attack Standard Evaluation BOard support file download site

http://www.risec.aist.go.jp/project/sasebo/

評価スキルの育成を目的に、測定が容易となるトレーニングボードも開発・整備中

新しい解析・対策手法の評価にも適しており、サイドチャネルの研究にも広く利用可能

対策を施した暗号LSIと，その有効性検証用に高精度の電力測定を可能とするSASEBO-RIIを開発

暗号回路を制御して電力を測定し，暗号鍵の解析を自動的に行うソフトウェアを開発

JST
CREST