耐タンパディペンダブルVLSIシステムの開発・評価

- 人為的攻撃による内部機密情報の漏洩・複製を防止するVLSIの実現 -

立命館大学，産総研，名城大学，三菱電機グループ

サイドチャネル攻撃対策を施した暗号処理回路

社会のディペンダビリティを支えているシステムではセキュリティ機能が重要

多くの場合，セキュリティ機能はLSIで実装されている

現在の情報化社会においてデータの暗号化は必須
暗号アルゴリズムは数学的には安全が保証

暗号アルゴリズムを知らなくても
容易に秘密情報の窃取が可能

サイドチャネル攻撃

二次情報（消費電力，電磁波）から
秘密情報を推定する解析法

- Differentical Power Analysis (DPA)
- Differentical ElectroMagnetic Analysis (DEMA)

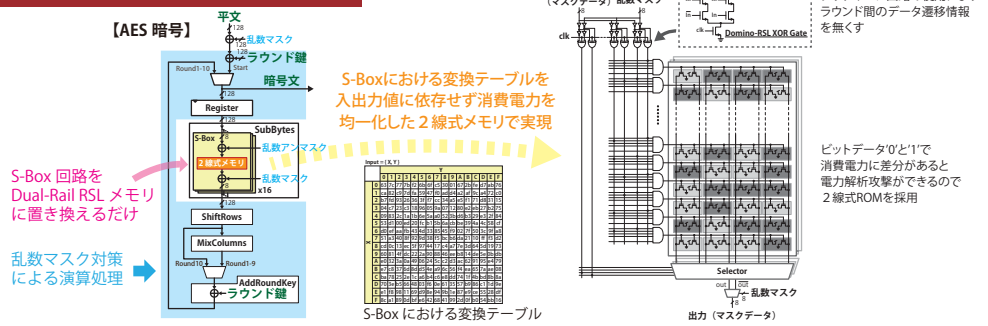
電力解析攻撃に耐性をもつ Dual-Rail RSL メモリ方式

電力解析攻撃に対する耐性を実現するために，
以下の対策を施した 2K ビットのメモリを使用

- 非線形処理である SubByte 変換処理を 2 線相補動作させ
  どのような入出力値に対しても消費電力を一定とする
- 他の線形処理は乱数によるマスキング対策により
  処理中のデータと消費電力との相関を隠す

提案方式の特長は実装の容易性，小面積，低消費電力

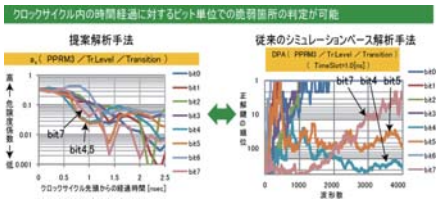
耐タンパメモリである Dual-Rail RSL メモリと
メモリ内部で使用する乱数発生回路を実装するだけで
電力解析攻撃の耐性を実現できる



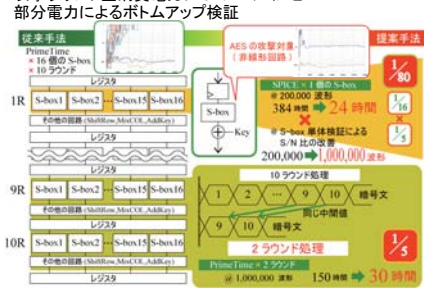
耐タンパ性検証 CAD

電力解析攻撃に対する脆弱性評価手法

➢従来の電力解析攻撃シミュレーションによって秘密鍵を推定するのではなく，どの箇所からリーク（秘密鍵に関連する情報）が多いかを評価する。

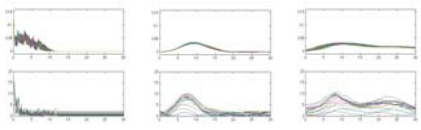


攻撃ラウンド型消費電力シミュレーションと部分電力によるボトムアップ検証



実機攻撃耐性予測

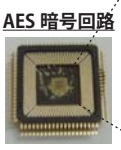
➢LSIシミュレーション電力に急峻なピークがあるような場合，積分効果により，実機上での観測波形を使ったほうが攻撃しやすくなる場合もある。そこで，シミュレーション電力波形から攻撃時に観測される波形を高速に予測することでより実際的な検証を実現。

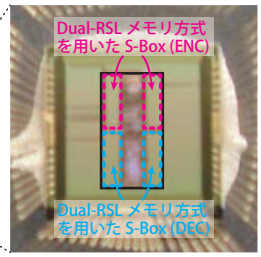


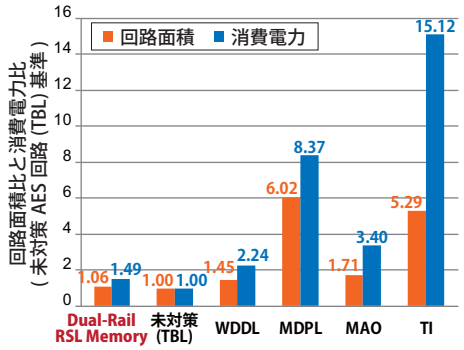
AES 暗号回路の試作及び他の対策方式との比較

- 提案手法である Dual-Rail RSL メモリ方式を AES 暗号回路に適用
- 0.18 μm CMOS プロセスを用いて設計・試作
- 設計時には開発した耐タンパ検証 CAD を使用

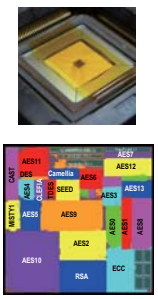
電源電圧	1.8 V
消費電力	24.3 mW
回路面積	[AES] 900,191 μm^2 [S-Box] 16,699 μm^2







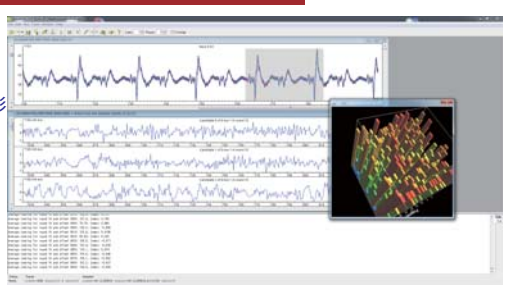
既存対策AES回路と比較
・WDDL ・MDPL
・MAO ・TI



電力解析攻撃評価結果（デモ）

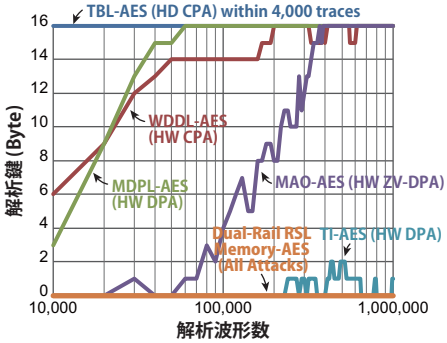
耐タンパ性能評価プラットフォーム
産総研開発：SASEBO-RII

取得波形



解析ツールとしてRiscure社INSPECTORを使用

評価結果



提案手法の安全性を実証

TI方式も耐性があるが，
問題は面積と消費電力

独立行政法人 科学技術振興機構 Japan Science and Technology Agency
CREST Core Research for Evolutional Science and Technology