暗号機器のサイドチャネル攻撃に対する安全設計に関する研究開発

（122308001）

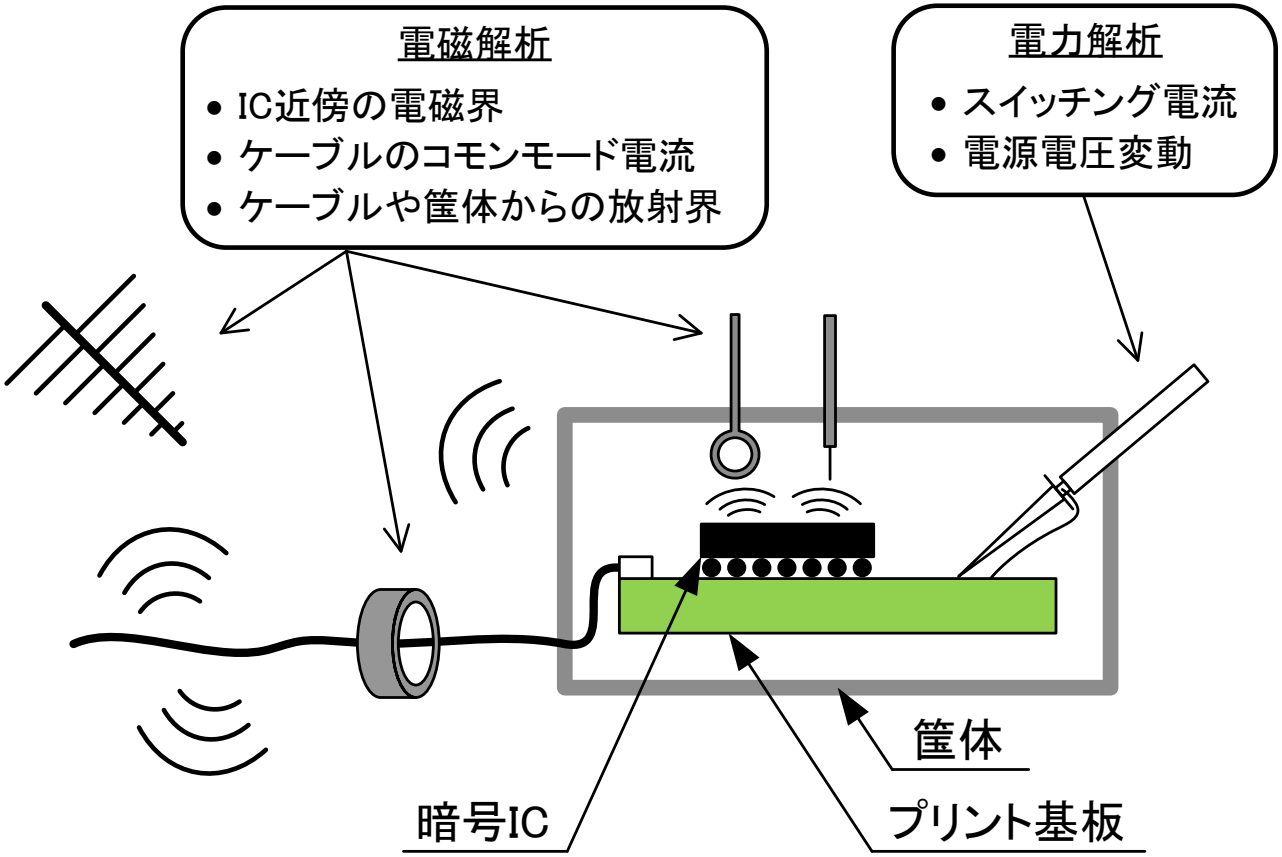
代表者：五百旗頭 健吾 (岡山大学)

分担者：豊田 啓孝, 野上 保之, 籠谷 裕人 (岡山大学)
渡辺 哲史 (岡山県工業技術センター)

ICTイノベーションフォーラム2014
2014年10月7日

背景：サイドチャネル攻撃

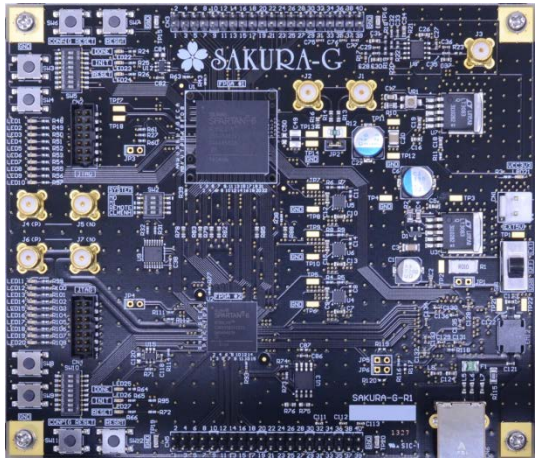
漏洩ノイズを利用した暗号解読の現実化

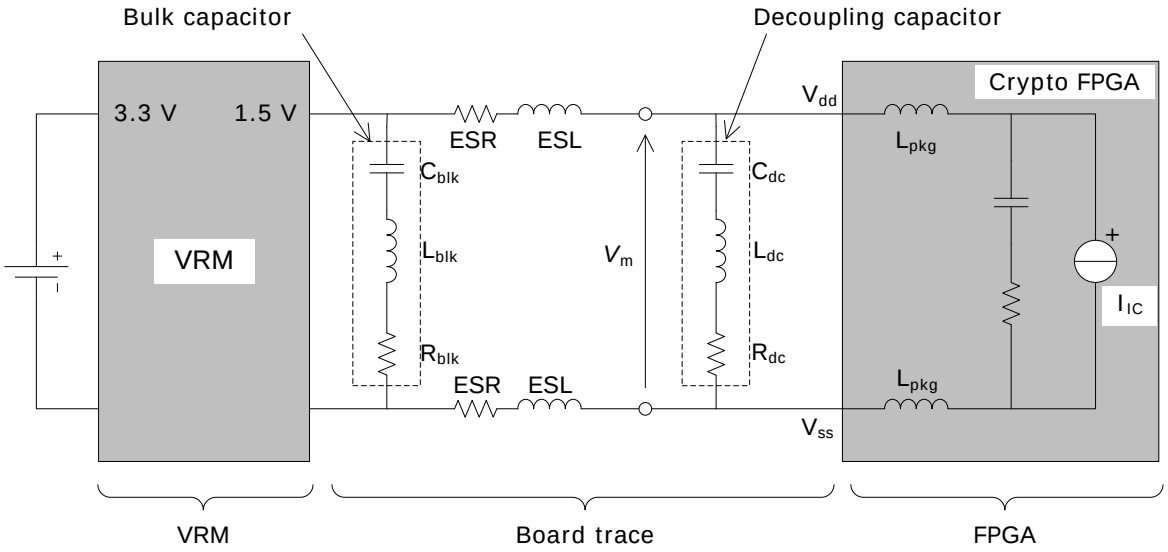


製品レベルでの対策設計が要求されるようになる

研究開発の内容

- サイドチャネル攻撃に対する安全設計の基盤技術開発
  - 等価回路モデルと回路シミュレーション

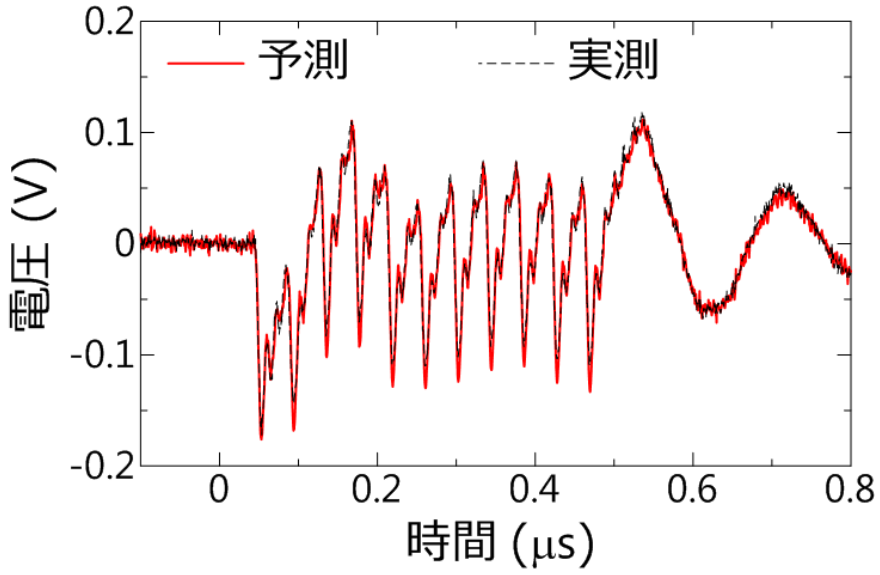




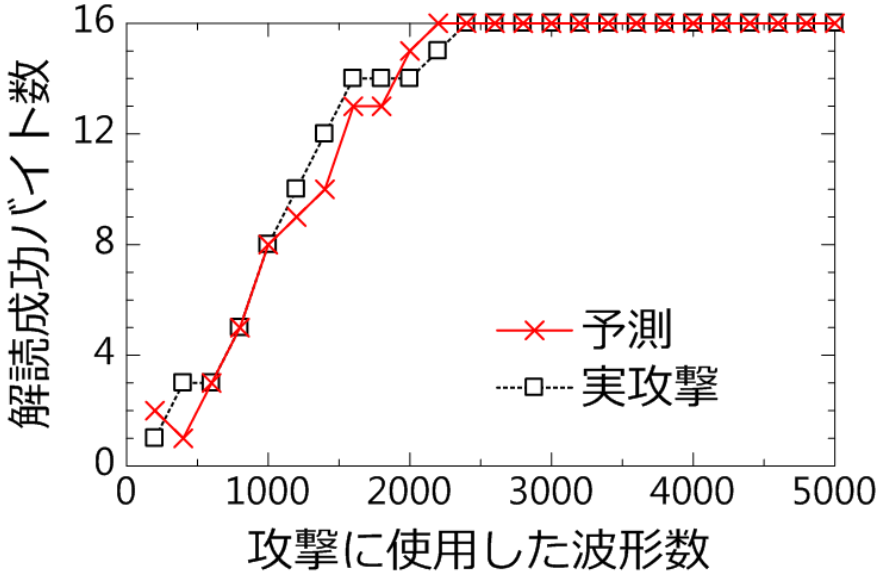
低コスト　高精度　高汎用性

研究開発の成果

サイドチャネル波形



攻撃コスト



- サイドチャネル攻撃の高精度予測を実現
- 安全性設計の基盤技術を開発完了

今後の取り組み

- 研究開発成果の展開
  - 標準評価プリント基板の開発
  - チップ回路設計レベルでのシミュレーション実現

- 波及創出効果への取り組み
  - 新たな耐タンパー暗号回路の開発