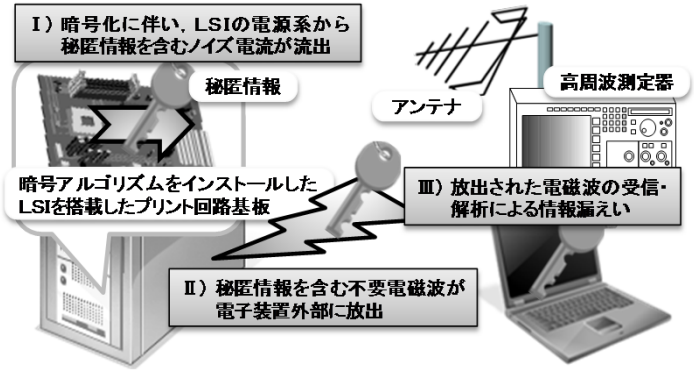
【参考1】　岡山大学　五百旗頭先生

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



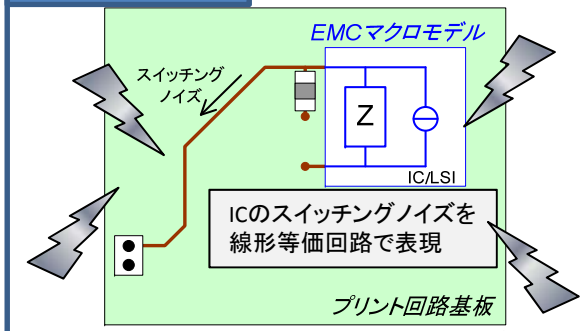
漏洩電磁波による情報漏洩（サイドチャネル攻撃）

問題点

- サイドチャネル攻撃が現実的脅威
- 試作前の安全性評価手法未確立
- 安全設計に大きなコスト
- 製品レベルでの安全性保証困難

既存技術

電磁環境技術の一つ



不要電磁波のEMCマクロモデリング技術

目的：　製品レベルでのサイドチャネル攻撃に対する安全設計のための基盤技術確立

研究開発の概要

① 暗号ICのEMCマクロモデル同定用プリント回路基板の作製
② EMCマクロモデルを用いた暗号ICの安全性シミュレーション
③ サイドチャネル信号源のSNR同定および標準評価指標としての有効性検証

期待される研究成果

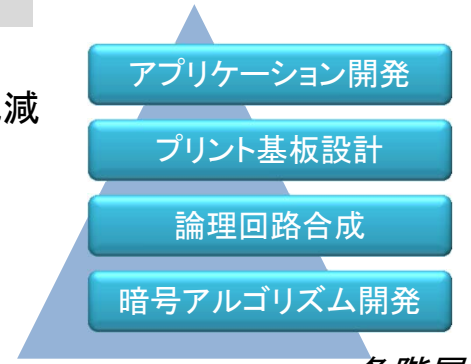
■製品レベルでの安全性シミュレーション手法確立
■暗号ICの安全性評価指標提案と同定法確立

技術的意義

■ 製品試作前の安全性シミュレーションの実現による開発コスト低減
■ 対策技術に関する研究開発の大幅な進展

社会的意義

■ サイドチャネル攻撃に対して安心・安全なICT製品の普及
■ 暗号技術を用いたICT機器の普及によるさらなる利便性向上および経済・社会活動のさらなる効率化



各階層の研究者が揃う

地域への貢献

■ 暗号機器に関する研究・人材育成拠点
■ 岡山におけるエレクトロニクス産業のポテンシャル向上

【参考１】　鳥取大学　川村先生

公共交通案内サービスにおける利用者行動の解析・活用技術の研究開発

バスネット：鳥取大学の開発する公共交通乗換案内サービス

Webブラウザ

ケータイ・スマートフォン

インテリジェントバス停

目的：乗換案内サービス「バスネット」利用者の行動解析を通して、公共交通利用者の希望や感じている問題を探り、路線バスの仕組みやバスネットの改良を推進

課題3：プライバシに配慮し収集

バスネット利用者の行動情報

課題1：解析システム開発

課題2：サービスを評価、改善

行動解析システムの改良

バスネットの改良

路線バスの改良

バスネット開発への応用
バスネットのユーザビリティを調査しシステムを改良

路線バスの改善への応用
利用者の真の需要を見極め、バス路線や時刻などを評価

研究課題1：大量の非定形データの収集、解析技術の開発
研究課題2：データに基づくバスサービス・バスネットサービスの評価手法の確立
研究課題3：利用者の安心と利便性のバランスの取れた行動情報収集技術の開発

期待される成果

公共交通分野におけるビッグデータ活用の技術開発
地域の公共交通サービス向上や人材育成
安心して利用できる行動履歴活用サービス技術の開発