FeliCa

「ディペンダブル VLSI 研究に求められるもの」
～セキュアチップFeliCaの視点から～

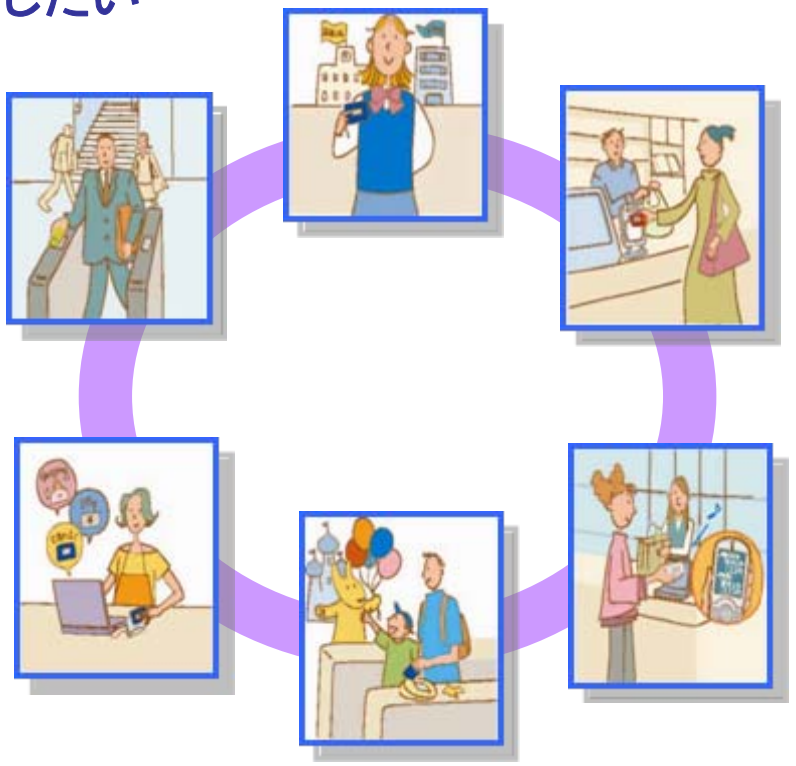
ソニー株式会社
B2Bソリューション事業本部・FeliCa企画開発部門
Chief Distinguished Engineer
要素技術開発部　統括部長　森田　直

SONY

セキュアアプリケーションからの要求

FeliCa

- 社員証
  - 成りすましを防ぎたい
  - 安全にバイオメトリクス情報を利用したい
- チケット
  - 権利の複製を防止したい
  - 安全に権利を移動したい
- クレジット
  - 成りすましを防止したい
  - 複製できないものがほしい
- 電子マネー
  - 残高を改ざんされると大変だ
  - **耐久性・信頼性がとても重要だ**
- 交通乗車券
  - 当然電子マネーと同様の**安心がほしい**
  - **故障、劣化しないものがほしい**



ディペンダビリティとセキュリティ

FeliCa

- 各品質要求とセキュリティの関係
  - 品質とは商品が持つひとつのサービス特性である
  - 信頼性、安全性、保全性、デザインは品質に含まれる
  - 意図的な攻撃にも耐える安心も組み込み真の信頼性を確保
- 品質に安心（セキュリティ）を組み込む時の課題
  - 「全ての機能は信頼できない」として疑う機能が必要
  - セキュリティを上げると保守性が損なわれる傾向にある
  - 真の信頼性を組み込むとコストが増大する傾向にある
  - セキュリティを上げれば信頼性と安全性も上がる
- VLSIにセキュリティ機能を組み込む時の課題
  - 適切な機能の組み込みには守るべき資産や脅威の想定が必要
  - 保守性が悪くなり顧客から見たサービス品質が悪化する
  - VLSIの開発費、期間、検査時間の増加、チップ面積が増大する

セキュリティを組み込むとは

FeliCa

- 狼狽しないVLSI *
  - クロック信号、リセット信号、電源線の動揺
  - レーザー光、イオン粒子、電磁界パルス、温度衝撃
- 漏洩させないVLSI
  - 漏洩電流、漏洩電磁界、漏洩時間
- 老練なVLSI
  - 全ての要求に真面目に反応しない
  - 詳細なステータスレスポンスの抑制
  - テスト機能の閉鎖
  - 自らを疑い再確認（プログラム、データ）
- 労力を必要とするVLSI
  - 素子配列スクランブル、蜘蛛の巣配線、ダミー配線
  - アクティブシールド、非同期クロック
  - アタッカーを混乱させるVLSIの動作

狼狽：Perturbation

要素技術として

FeliCa

- ミックスドシグナルOne Chip IC技術
- 動作電力抑制技術
- 真性乱数発生とその高速検証技術
- 信頼性の高い不揮発性メモリ技術
- ロジックのオファスケーション(Obfuscation)
- 非同期回路設計ツールと回路の効率化
- 形式的手法基づく組み込みソフト設計
- セキュアソフト設計ルール
- VLSI認証機能
- 耐タンパ機能（アナログ、デジタル）

＊暗号技術は既存の検証された方式が前提

まとめ

FeliCa

- ディペンダビリティが測定できれば製品利用の拠り所が決まる
- 高すぎるディペンダビリティ要求は高価な商品につながるが、電子マネーでは要求が必然的に高くなる
- 適切な要求に合わせるための研究
  - ロジックのオファスケーション用EDAツール
  - 破壊モードとディペンダビリティの関係
  - ディペンダビリティを維持するリアルタイム機能検証技術
  - ディペンダビリティを検証しやすい耐タンパ機能
- 「セキュリティとディペンダビリティの融合」
  - 日本学術会議・情報セキュリティ委員会の
    セキュリティ・ディペンダビリティ分科会の提言がある