耐タンパディペンダブル VLSIシステムの開発・評価

～機器認証機能のための セキュリティコンポーネント～

立命館大学・産総研・名城大学・三菱電機

発表内容

- 暗号技術とLSI
- チップセキュリティの問題設定
- セキュリティコンポーネント
- まとめ

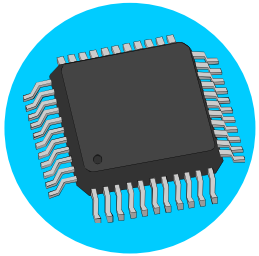
暗号技術とLSI

- 様々なシーンで利用されるセキュリティ機能 ～社会インフラから組み込み機器～

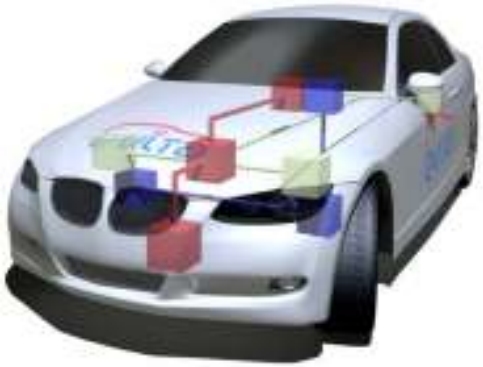
高速道路料金収受システム（ETC）

スマートカード

バッテリ



セキュリティ機能は
LSIで実現



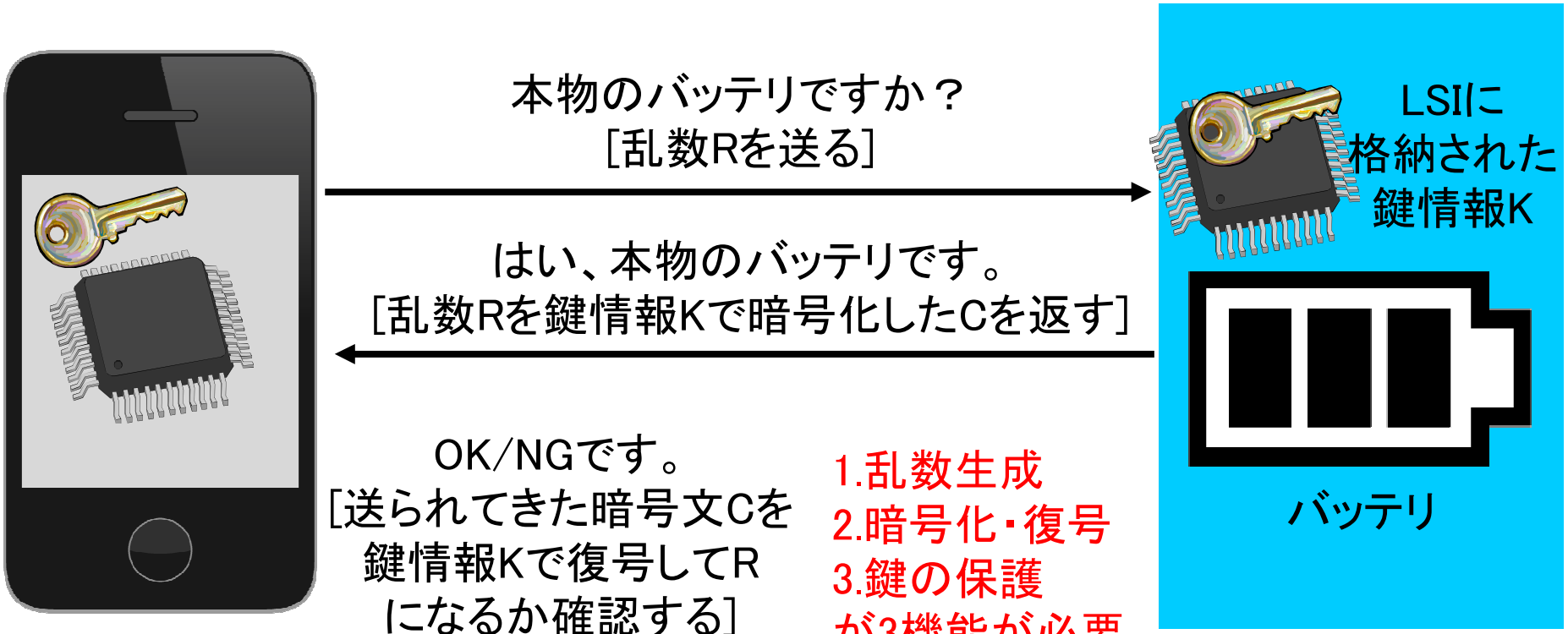
Car Security（e.g EVITA Project）

ゲーム機

スマートメータ

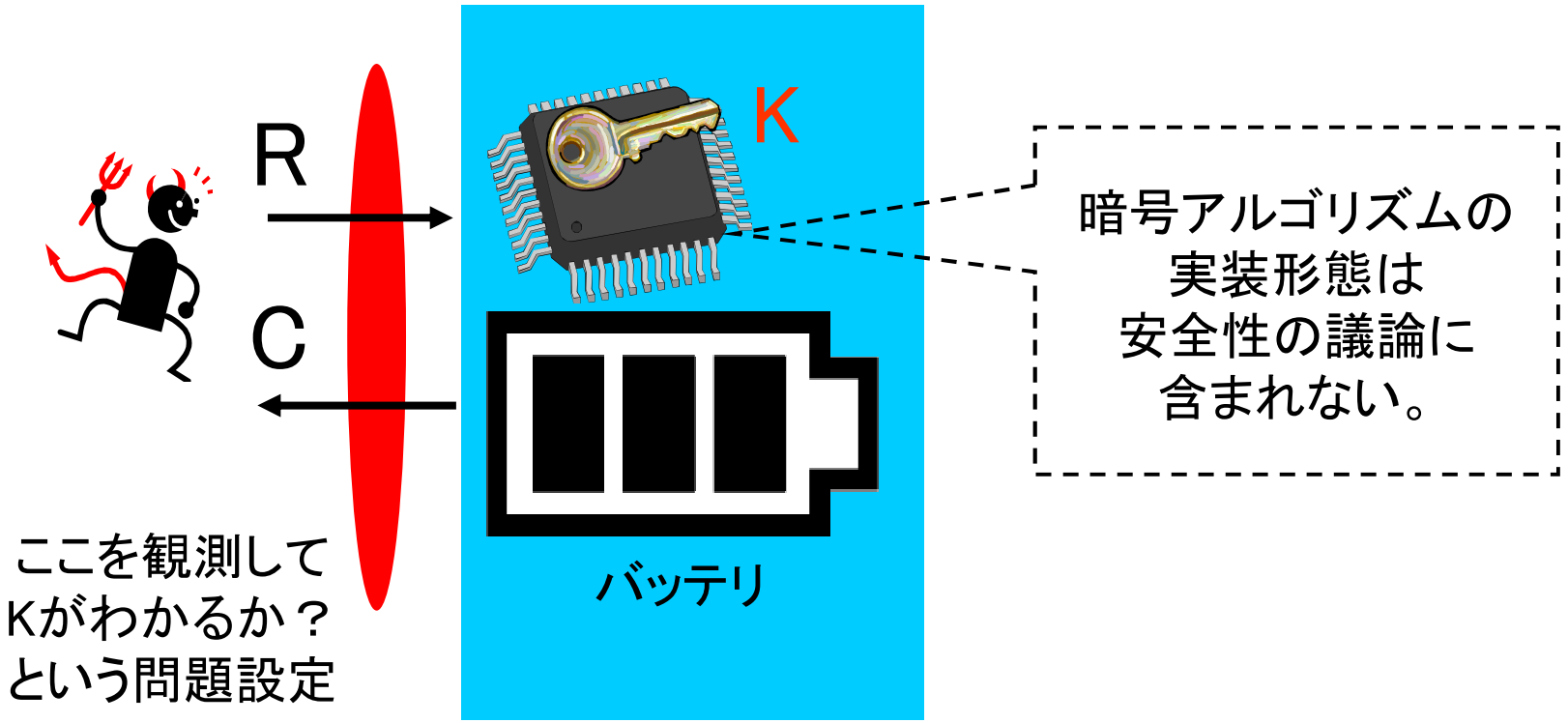
バッテリ認証

- **典型的な「純正品」であることの認証方法**
  - ・秘密の鍵情報Kを互いに開示することなく、共有していることを確認する。
  - ・質問の内容を乱数を使って毎回変えているのがポイントである。
  - ・下図は共通鍵暗号方式を使った例。公開鍵暗号方式を使うと、本体側に秘密情報を保持しなくてよくなるが、処理速度が10～1000倍程度遅くなる。



暗号アルゴリズムの安全性

- **暗号アルゴリズムの安全性**
  - ・入力Rとそれに対応する出力Cをたくさん集めても、鍵情報Kがわからないことを評価するのが、「暗号アルゴリズム」の安全性である。
  - ・入力R、出力Cは「通常のチャネル」から得られる情報と定義される。

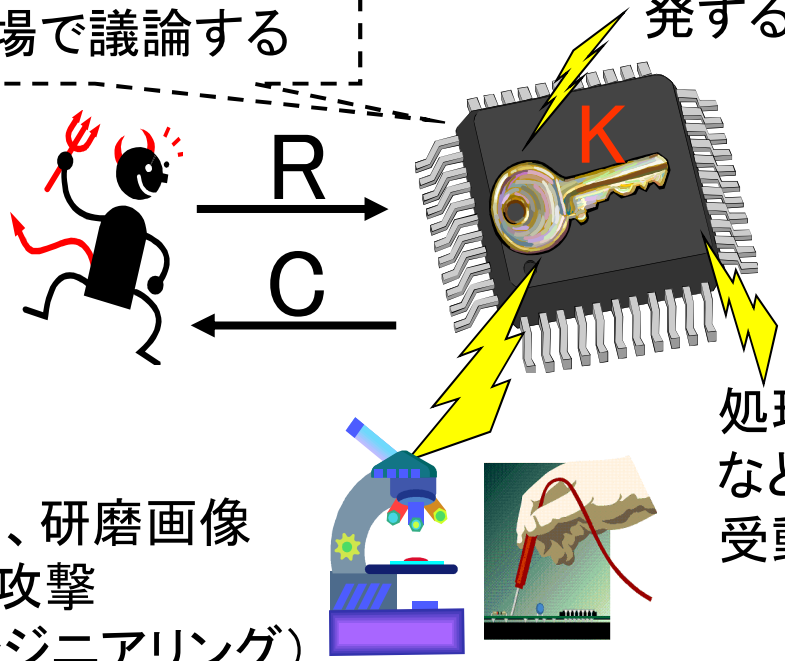


チップセキュリティの問題設定

- **LSIの「耐タンパ性」を議論する問題**
  - ・暗号アルゴリズムの入出力情報に、考えうる手段で得られる情報を追加して安全性を議論する。
  - ・スマートカード用のセキュリティチップでは、この安全性に関する第3者評価が必須である。

LSIに様々な作用を加え、様々な物理量を観測できる立場で議論する

電源、クロックへのグリッチ挿入、裏面からのレーザ照射などによって誤動作を誘発する能動攻撃（フォルト攻撃）



処理時間、消費電流、漏洩電磁波などサイドチャネル情報を用いた受動攻撃（サイドチャネル攻撃）

ナノプローバ、FIB、研磨画像などを用いた破壊攻撃（HWリバース・エンジニアリング）

チップセキュリティが破られた事例紹介

「良くできた」暗号アプリほど、weakest linkがチップセキュリティになる。

- On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme @CRYPTO2008
  キーレスエントリー用チップに対するサイドチャネル攻撃。認証鍵だけでなく工場鍵まで取れるため、クローンの作成が可能となった。

- Deconstructing a 'Secure' Processor @BlackHat2010
  インフィニオンのTPMをリバースエンジニアリングにより鍵抽出。ただし、TPMは公開鍵暗号でシステム構築されるため、攻撃がそのチップにしか影響しない。

- Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World @CHES2011
  NXPの非接触ICカードチップがサイドチャネル攻撃により破られる。

- On the Portability of Side-Channel Attacks – An Analysis of the Xilinx Virtex 4, Virtex 5, and Spartan 6 Bitstream Encryption Mechanism @CT-RSA2012
  Xilinx社のFPGAに搭載されているビットストリーム暗号化機能をサイドチャネル攻撃で解除。

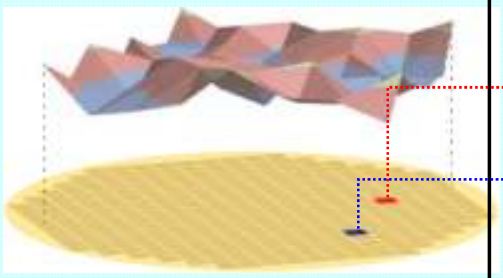
- Breakthrough Silicon Scanning Discovers Backdoor in Military Chip @CHES2012
  Microsemi社のProASIC3に設定可能なJTAG認証鍵をサイドチャネル攻撃で抽出。
  さらに、JTAGのリードバック保護機能にはバックドアがあり、その認証鍵も抽出。

Physical Unclonable Function

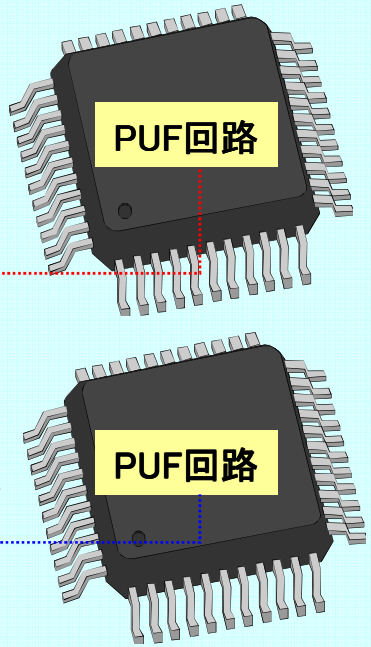
【PUF方式】

入力

0xEF01 A332 1551



ウェハ



デバイス固有の応答

0xC3E6 6520 311A 4965 90C7 0430 0891 ED46

0x9A1F 5433 3653 A8F7 25EF D151 8F5C D05F

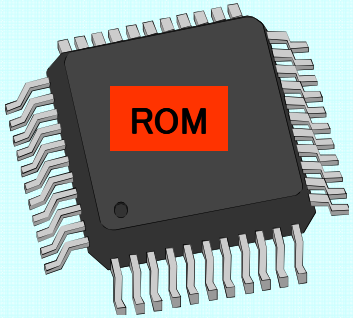
全く同じ回路から異なる値が出力される

- 同一入力をLSI 与えても内在する製造ばらつきはチップ毎に異なるため出力信号はチップ毎に異なる
- 製造ばらつきを人工的に制御・複製するのは困難

【従来方式】

秘密情報（暗号・認証情報 etc.）

メモリに書き込み



不揮発領域に秘密情報（ID）を保存
電源OFF時も秘密情報残存
リバースエンジニアリングによる解読の危険性

PUFを用いた機器認証

機器認証には「乱数」、「暗号化・復号」、「盗めない鍵」が必要、

1．物理乱数発生回路

乱数

乱数（平文）

乱数を認証鍵で暗号化して送り返す

暗号文

2．復号回路

2．暗号化回路

暗号文を認証鍵で復号してもとの乱数に戻るか確認する

暗号アルゴリズムで守られる

見えないから盗めない

3.PUF回路

認証鍵

消える鍵

認証鍵を取り出す

3.PUF回路

認証鍵

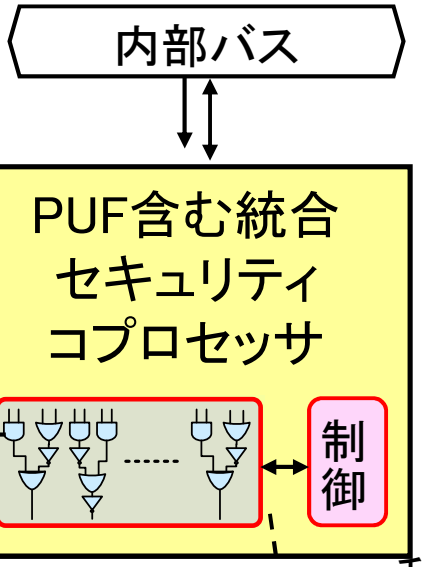
消える鍵

認証鍵を取り出す

セキュリティコンポーネント

本プロジェクトで開発したセキュリティコンポーネントの例

【統合セキュリティコプロセッサ】

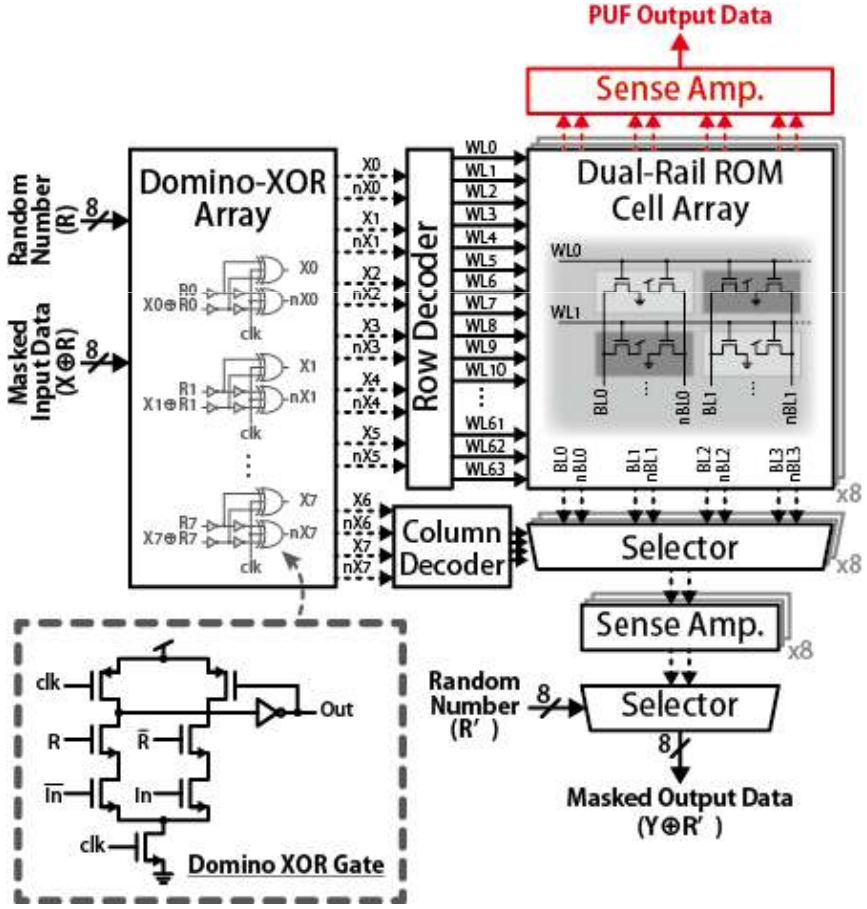


1. 暗号化・復号機能
2. 物理乱数生成
3. PUF(ID生成)

の3機能を統合

乱数性は
世界標準のテスト
(SP-800)をパス

【サイドチャネル対策AES】
(IO-Masked Dual-Rail ROM)



K. Shimi u, D. Su uki, T. Tsurumaru, T. Sugawara, M. Shio aki and T. Fujino: Unified Coprocessor Architecture for Secure Key Storage and Challenge-Response Authentication. IEICE Transactions 97-A(1): 264-274 (2014)

まとめ

- 本発表では、チップセキュリティを実現するためのセキュリティコンポーネントについて紹介
- 暗号アプリケーションでLSIは秘密情報の保管庫として、重要な役割を担っている
- システム複雑になり、かつプレイヤーが増えると鍵管理が重要な課題になる。
- 暗号機能は演算が正しく動作するだけではテストとして不十分。理想的には、第3者による侵入テストが望ましい。（例：コモンクライテリア）
- より重要なのは、上位設計でリスクとセキュリティ機能の要件と、達成すべきセキュリティレベルを明確にすること。