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

情報処理システムが抱える脅威

情報化社会を支える組込システムは今現在も増加傾向にある一方で情報漏洩，情報改ざん，偽造複製などの脅威にさらされている
例えば，自動車もスマートフォン等の様々な外部システムと繋がろうとしており，新たな脅威に備える必要がある

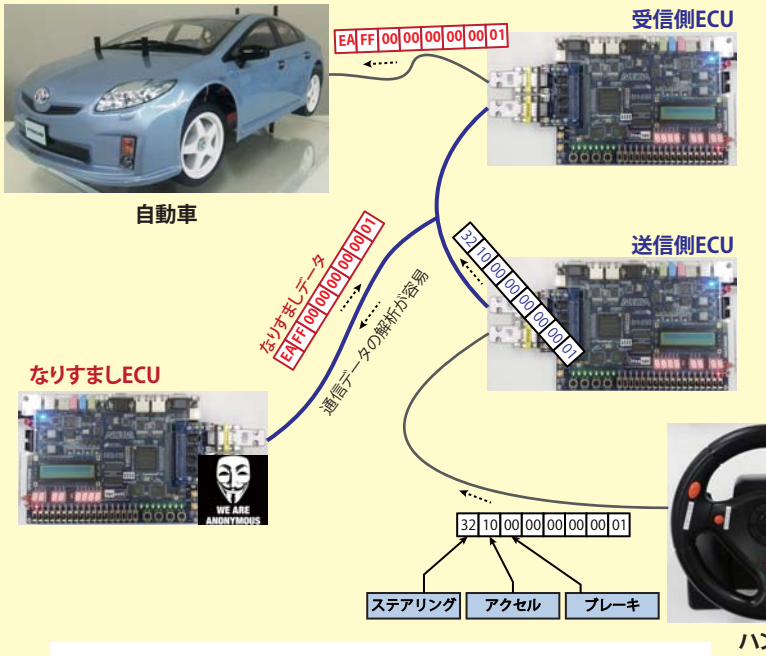
➡ **情報処理システムにはセキュリティ技術は必要不可欠**

自動車の乗っ取りデモ

＊本デモンストレーションの開発には名古屋大学の組込みリアルタイムシステム研究室の本田准教授，
附属組込みシステム研究センターの倉地助教のご協力を頂きました．

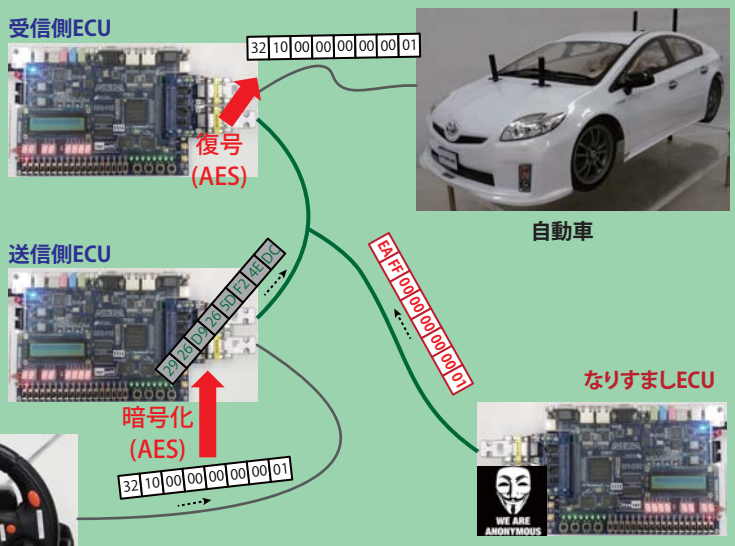
業界標準のOS　AUTOSAR仕様のToppers/ATK2上で動作するセキュリティSW/HWを開発

通常の CAN 通信



CAN通信では，通信データの暗号化や通信相手との認証を行っていないため，通信データが容易に解析でき，なりすましECUからの誤った判断や指示を受け取ってしまう危険性がある

AES 暗号化 CAN 通信



通信データの暗号化や通信相手との認証を行い安全に走行

(長所) 乗っ取り回避
　暗号通信により通信データの解析が困難
(短所) 暗号処理による遅延
　AES暗号は128bit長のブロック暗号のため
　２パケットの通信が必要

サイドチャネル攻撃と侵襲攻撃による脅威

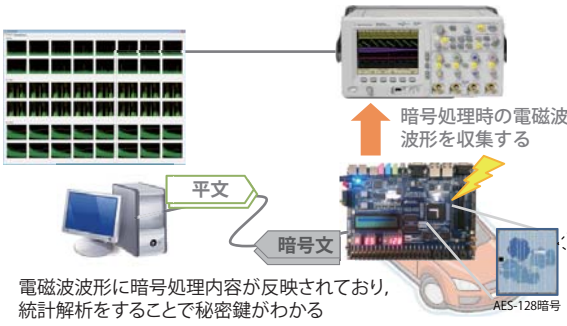
暗号化ハードウェアを用いる際，サイドチャネル攻撃と侵襲攻撃（物理的攻撃）に対する対策は欠かせない

- **サイドチャネル攻撃により電子機器，半導体製品から秘密情報（暗号鍵）が窃取される危険性**

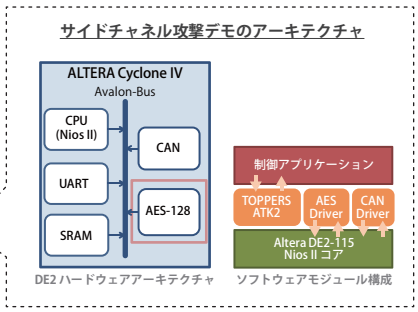
サイドチャネル攻撃デモ

漏洩電磁波を用いたサイドチャネル攻撃
（電磁波解析攻撃）

市販の FPGA ボードで動作する
AUTOSAR 仕様の車載 OS 上で
CAN 通信の暗号化を実行
→ CAN 通信路の情報と電磁波プローブ
　を用いて暗号鍵の窃取はできる



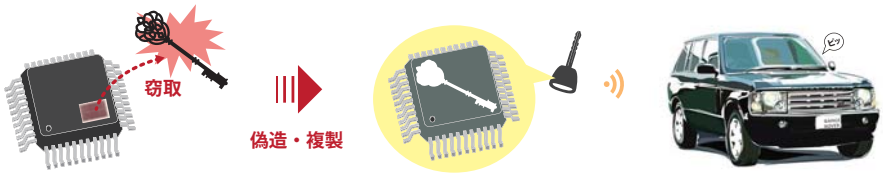
電磁波波形に暗号処理内容が反映されており，
統計解析をすることで秘密鍵がわかる



- **不揮発性メモリ上の秘密情報（暗号鍵）は物理的攻撃により窃取される危険性**

キーレスエントリを模したデモ

複製鍵による自動車盗難と PUF 技術を用いた対策



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

連絡先：立命館大学　藤野 毅
Tel　：077-561-5150
E-mail：fujino@se.ritsumei.ac.jp

耐タンパディペンダブルVLSIシステムの開発・評価

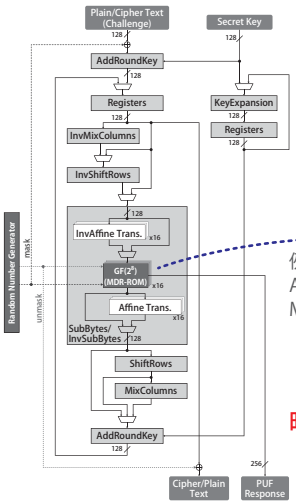
- 人為的攻撃による内部機密情報の漏洩・複製を防止するVLSIの実現 -

立命館大学，産総研，名城大学，三菱電機グループ

IO-Masked Dual-Rail ROM 方式を用いたサイドチャネル攻撃対策と Physical Unclonable Function (PUF) を用いた偽造・複製防止技術

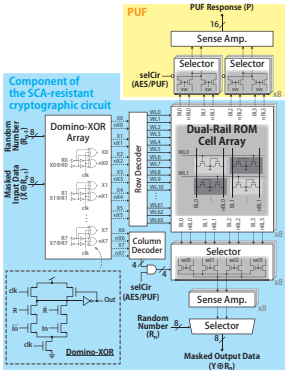
IO-Masked Dual-Rail ROM (MDR-ROM) を用いたサイドチャネル攻撃対策

主な，サイドチャネル攻撃のターゲットとなる非線形回路を MDR-ROM に置き換え，
乱数マスクのための乱数発生回路を加えるだけでサイドチャネル攻撃対策が実現できる
加えて，偽造･複製防止技術と期待される PUF としても利用可能



- サイドチャネル攻撃対策と PUF 技術を ROM で実現
  → 小面積・低消費電力
- メモリを用いた一般的な設計手法で対策が可能
  → 実装が容易
- 様々な暗号に本手法は適用可能

例）
AES 暗号回路内の GF(2^8) 演算を
MDR-ROM で実現

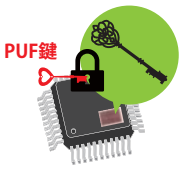


100 万波形を用いても
暗号鍵の窃取に成功せず

PUF 技術を用いて秘密情報を管理

Physical Unclonable Function (PUF) :
ランダムな製造時のばらつきからチップ固有情報を生成する技術

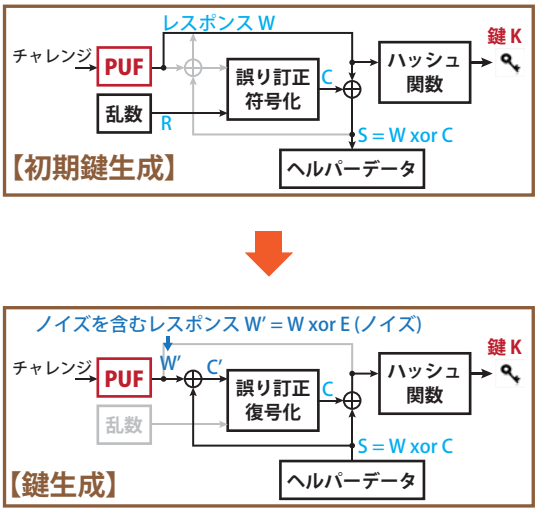
- 同一入力信号（チャレンジ）を与えても，内在する製造ばらつきはチップ毎に異なるため出力信号（レスポンス）はチップ毎に異なる
- 製造ばらつきを人工的に制御・複製するのは困難
- 暗号化や認証時に必要な時にしか生成されない



PUF 技術から暗号鍵を生成して秘密情報を暗号化（使用チップでしか復号化できない）

PUF のレスポンスから暗号鍵を生成する際の技術課題

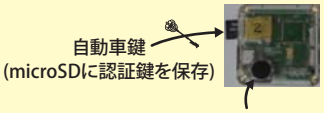
PUF では製造ばらつき情報という微少な差異を利用しているために出力が安定せず，そのままでは同じ暗号鍵を得るのは困難である．そこで，誤り訂正を用いて安定した鍵生成を行っている．



ヘルパーデータからは暗号鍵は推定できない

【デモンストレーション説明】
サイドチャネル攻撃対策 AES 暗号と PUF を組み合わせたセキュアシステム

PUF 無し

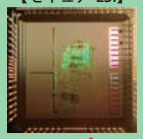


キーレスエントリーを模した
デモンストレーション

鍵データ
窃取

microSD（認証鍵データ）が
窃取（コピー）されると車の
扉は開いてしまう
結果として自動車も盗まれる

PUF 有り



Hybrid Masking Dual-Rail ROM 方式による
サイドチャネル攻撃対策 AES 暗号回路と
PUF 回路を搭載したセキュア LSI により
自動車の認証鍵データを防御

鍵データ
窃取

microSD 内の認証鍵データは
PUF 鍵で暗号化され守られている
たとえ，認証鍵が窃取されても自動車の扉は解錠できない
PUF 鍵は LSI 固有なので複製されても同一鍵は生成されず安全

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

連絡先：立命館大学　藤野 毅
Tel　：077-561-5150
E-mail：fujino@se.ritsumei.ac.jp