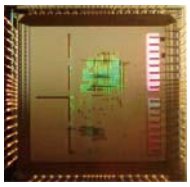





ネットワークLSIシステム 研究室紹介

応用演習

2016.10.03

教授　藤野　毅

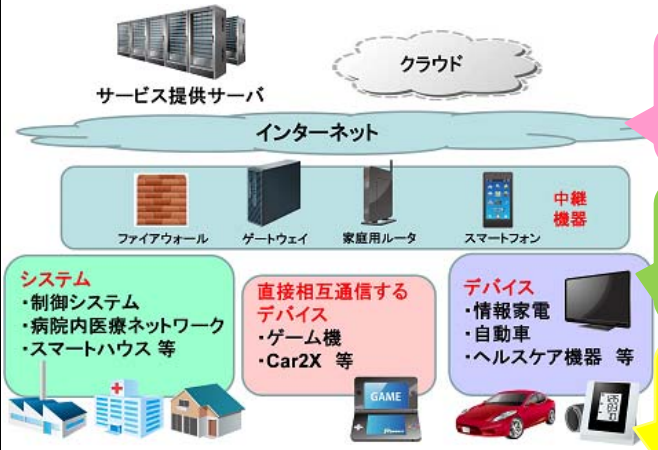
ネットワークLSIシステム研究室紹介

- 設立：2003年4月
- 研究テーマ
  - 特徴あるLSIアーキテクチャを使ってネットワーク＆セキュリティーシステムへ応用する研究をしています
  - 特に最近はIoTセキュリティを主たる研究テーマにしています
- 研究室メンバー
  - 教授：藤野　毅
  - 研究教職員
    - 准教授（常勤）：白畑　正芳，汐崎　充，
    - 研究員（常勤）：久保田貴也
    - 秘書：松田　詩織，清水　明恵
    - 客員研究員（非常勤）：熊本　敏夫（大阪産業大学）
  - (M2)：6名，(M1)：4名
  - 学部学生：12名（7名がM1に進学予定）

IoTとは？

RITSUMEIKAN NTSOC LAB. 3

■ 「IoT」とは「Internet of Things」の頭文字を取った単語で，一般的に「モノのインターネット」と呼ばれている．IoTを簡単に説明すると、「身の周りのあらゆるモノがインターネットにつながる」仕組みのこと．



農業応用
農地に取り付けたセンサーで読み取った日射量や土壌の状況をもとに、水や肥料の量を制御

医療応用
着用型ウェアラブルデバイスによる健康状態の記録・管理、医師との共有

自動運転システム
自動車が自動車同士または周囲のインフラや歩行者と通信して，安全走行

https://www.ipa.go.jp/security/iot/iotguide.html より引用

IoTのセキュリティ事例（1）

RITSUMEIKAN NTSOC LAB. 4

■ 産業・事務機器
- ネット接続の複合機　蓄積データが丸見え状態に
- ネットワークカメラをハッキング　赤ん坊に「起きろ！！」とリモートから罵声

■ 自動車関連
- 遠隔操作で自動車制御を乗っ取り　走行中の急ブレーキで事故誘発
- 狙われた自動車のスマートキー　脆弱性対策が後手に回る
- 遠隔イモビライザーを不正使用　イモビライザーの乗っ取りも

日経BPイノベーションICT研究所　編
A4変型判〔CD-R付〕296ページ
価格　：　32,400円（税込み）
読者特価　：　27,000円（税込み）
ISBN　：　978-4-8222-3780-6
発行元　：　日経BP社
発行日　：　2016/06/27

IoTのセキュリティ事例（2）

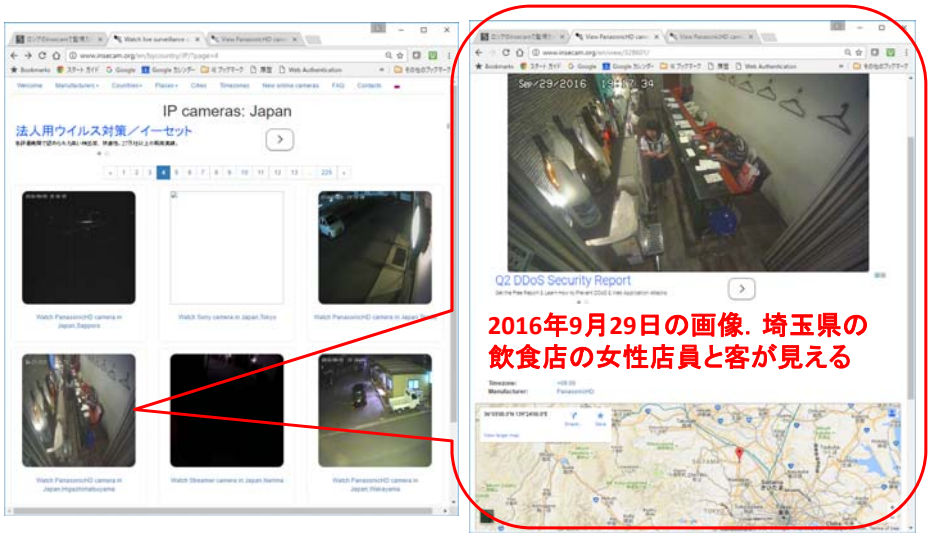
RITSUMEIKAN NTSOC LAB. 5

- 家電機器
  - スマート冷蔵庫に脆弱性　ログイン情報のぞかれる可能性
  - ハッキングチップ内蔵の中国製アイロン　ロシア税関で発見される
- 公共機器
  - ホテルの電子錠を小型デバイスで開錠　400万室以上に進入可能な脆弱性
  - 道路案内表示板をハッキング　「ゾンビ注意」などに変更
  - 14歳の少年がATMに進入　SMSを使った現金引き出しも
- 医療機器
  - 心臓ペースメーカを不正操作　電気刺激装置では致死量の電流を流す
- 防御機器？
  - 自動照準のスマートライフル　ハッキングで誤射の可能性

漏えいするWebカメラデータ

RITSUMEIKAN NTSOC LAB. 6

- ロシアの「Insecam」というサイトで，日本の1350の監視カメラ画像がリアルタイムで表示できる.



自動車のハッキング事例

RITSUMEIKAN NTSOC LAB. 7

■ 2013年8月米ラスベガスで開催のハッカーの祭典「デフコン」で、トヨタ自動車のプリウスなどを例に専門家が手法を披露

ミラー氏らは車載ソフトの解析で接続に成功。運転手の意思に反して急加速やブレーキを利かせたり、ハンドルを動かしたりしたほか、エンジンを切り、残り少なかった燃料計を満タンとして表示させる様子などを映像とともに披露
車載ネットワークへの物理的侵入を必要とした

http://www.huffingtonpost.jp/2013/08/04/car_hakking_n_3705303.html より引用

現在行っている様々な研究

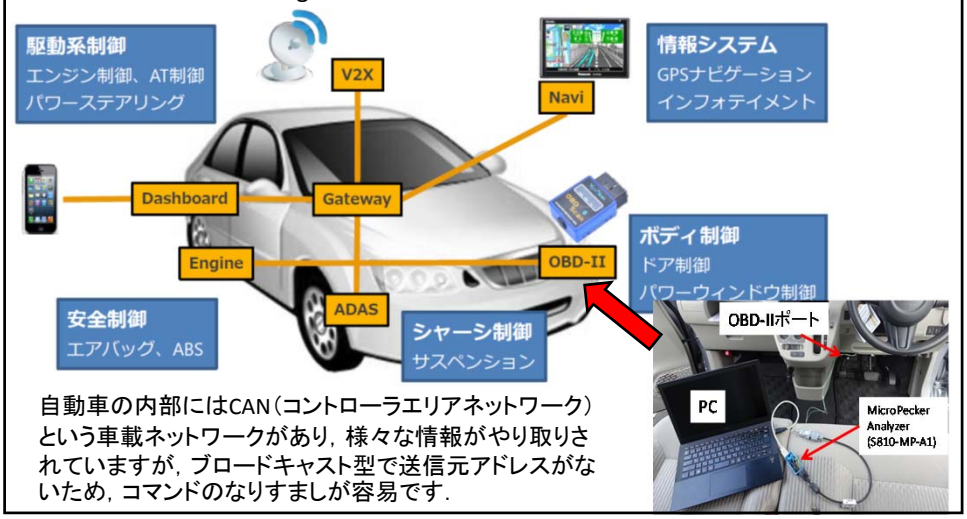
RITSUMEIKAN NTSOC LAB. 8

- (1) 実車ハッキング実験
- (2) ソナーセンサへの攻撃基礎実験
- (3) 赤外線と可視光画像の比較
- (4) ラズパイ版GSSE監視カメラ
- (5) CMOSイメージセンサPUF
- (6)サイドチャネル攻撃

（1）自動車内への侵入経路

RITSUMEIKAN NTSOC LAB. 9

- 外部との通信は以下のように複数存在する
  - 車載整備用OBD－IIポート，V2X（車と車，車とインフラ間等）通信ユニット，カーナビゲーションシステム，車載WiFiシステム
  - OBD（On Board Diagnostics）-IIは自己診断機能のためのポート



自動車の内部にはCAN（コントローラエリアネットワーク）という車載ネットワークがあり，様々な情報がやり取りされていますが，ブロードキャスト型で送信元アドレスがないため，コマンドのなりすましが容易です．

（1）実車ハッキング実験＠立命館大学

RITSUMEIKAN NTSOC LAB. 10

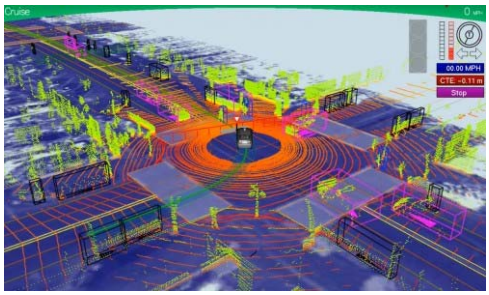
- 大学院生が，自動車を2015年9～10月，解析して行いました．
- ワイパーやウインカーをPCから遠隔動作もできます．

グーグルの自動運転車

RITSUMEIKAN NTSOC LAB. 11

- われわれの自動車は、常に十数台が路上を走っていて、このほど30万マイル（約48万km）以上のテスト走行を完了した。テストはさまざまな交通状況で行われ、コンピュータ制御下において事故は1度もなかった。(2012)
- 視覚障害を持つ男性がショッピングに行くシーン
  http://www.google.com/about/jobs/lifeatgoogle/self-driving-car-test-steve-mahan.html

グーグル自動運転車

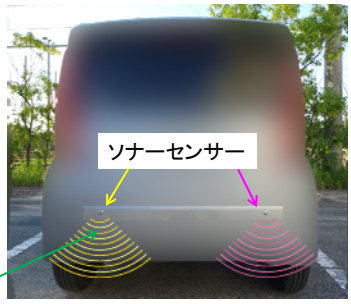


グーグルカーが処理しているといわれるデータ

（2）ソナーセンサーに対する攻撃

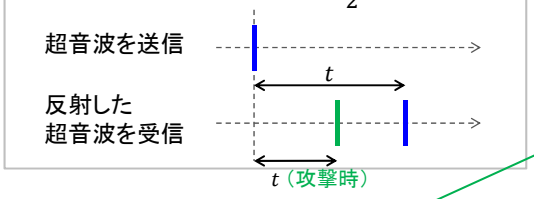
RITSUMEIKAN NTSOC LAB. 12

ソナーセンサ：
近距離の障害物を検知するために普及



測距原理

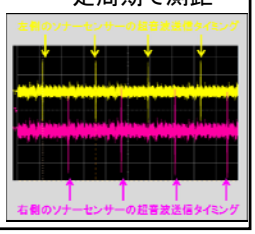
Time of Flight方式　$L = c \times \frac{t}{2}$　（c：音速）



攻撃者

偽の超音波を送信

一定周期で測距



攻撃シナリオ

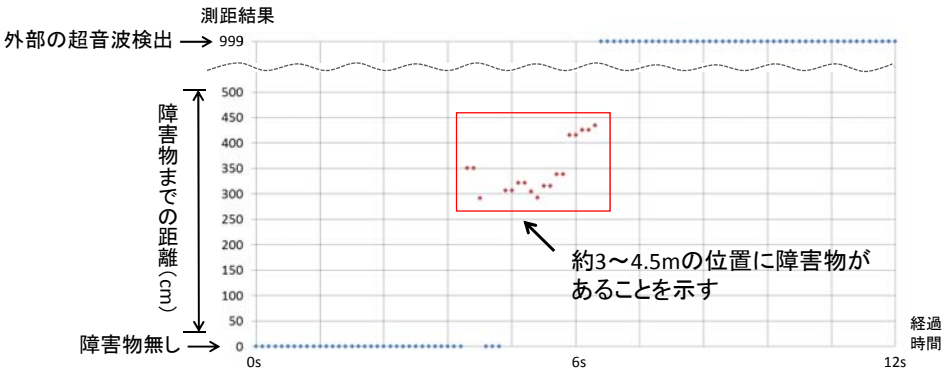
- 反射した超音波になりすまして偽の超音波を受信させる
  ⇒ 測距値の改ざん攻撃
- 反射した超音波を検知できない状態とする
  ⇒ DoS（Denial of Service）攻撃

（2）測距値の改ざん攻撃＠立命館大学

RITSUMEIKAN NTSOC LAB. 13

- 2016年3月卒業者の修士論文に内容記載（テスラ発表前）
- ソナーセンサーが測距を行うタイミングに合わせて，偽の超音波を送信
- テスラのように距離表示がないため，車載CAN情報で読み取り

⇒ 一時的ではあるが，障害物までの距離が観測された

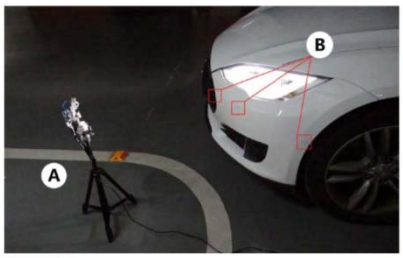


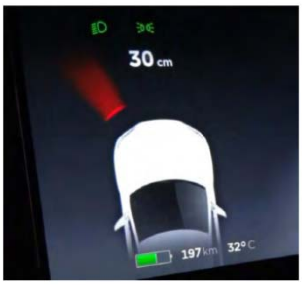
センシング段階での測距値の改ざんが可能であることを示した

（2）自動車のセンサーへの攻撃

RITSUMEIKAN NTSOC LAB. 14

- テスラに搭載された超音波センサへの攻撃
- 2016年8月Defcon 浙江大学の発表





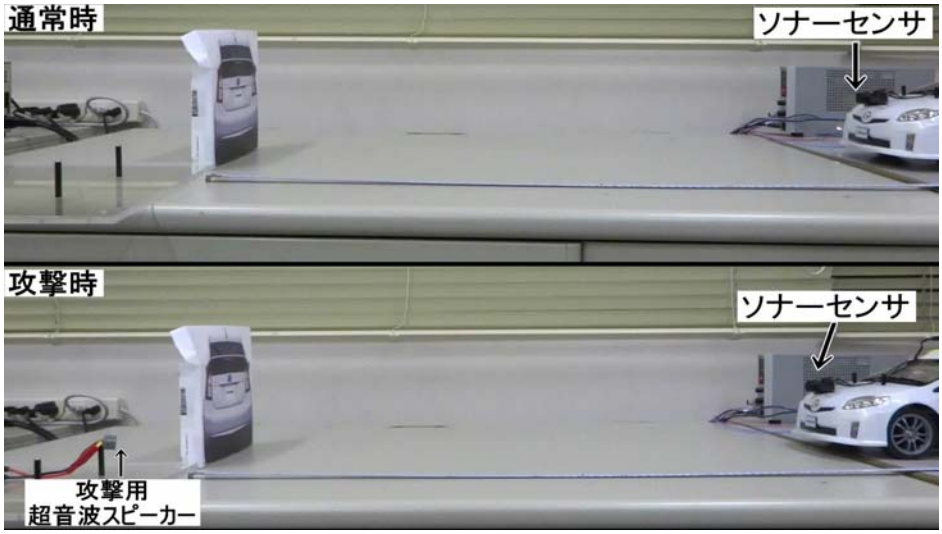
Tesla Normal　　Tesla Jammed　　Tesla Spoofed

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles.pdf より引用

（2）測距センサーへの攻撃デモ＠立命館大学

RITSUMEIKAN NTSOC LAB. 15

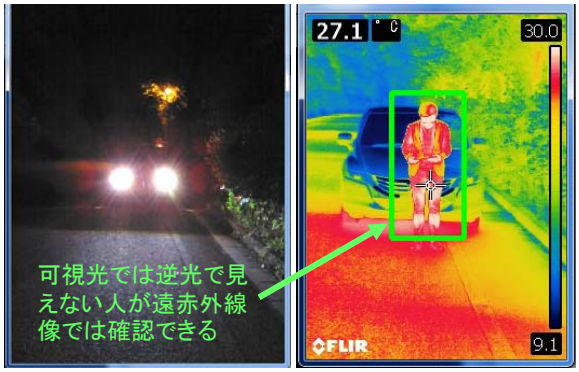
- 超音波測距センサーを用いた衝突防止ブレーキデモ実験模型自動車を試作
- 超音波スピーカを用いて，測距センサーをDoS攻撃するとブレーキ作動不能に



（3）赤外線と可視光画像を併用

RITSUMEIKAN NTSOC LAB. 16

- 赤外線カメラの実験
  - 夜間，ヘッドライトで見えなくなっていた人物が赤外線カメラでは検出可能！

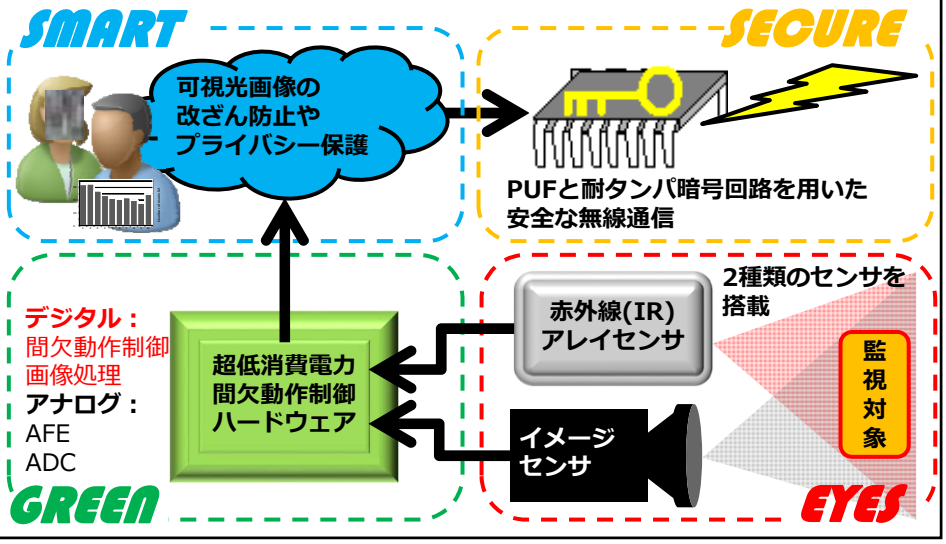


可視光カメラ画像　　遠赤外線カメラ画像

（4）GSSE監視カメラ

RITSUMEIKAN NTSOC LAB. 17

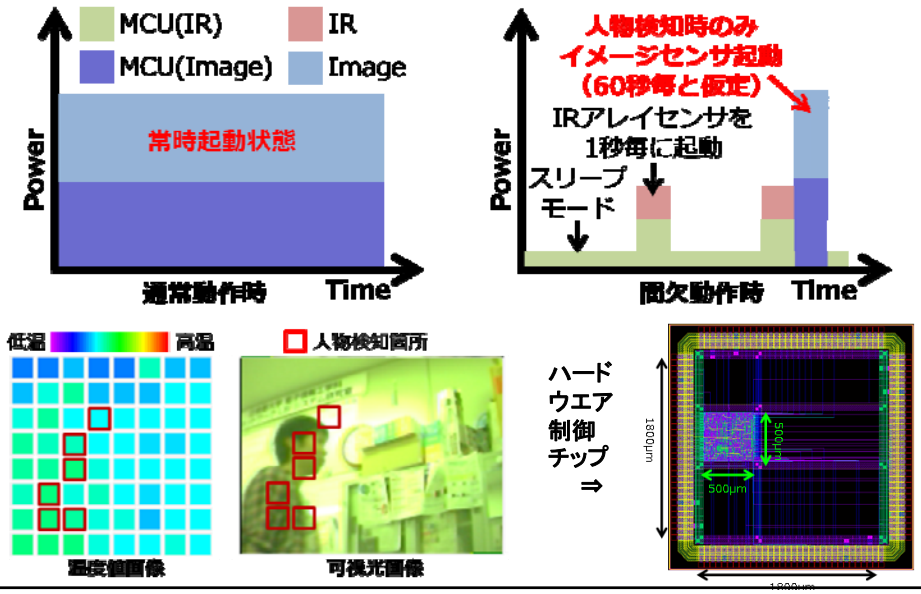
■低消費電力（単3電池2本）で2年連続動作，プライバシーを保護できる監視カメラ



（4）間欠動作による消費電力削減

RITSUMEIKAN NTSOC LAB. 18

■GSSEのコンセプトと試作チップ



（4）ラズパイ版GSSE監視カメラシステム

RITSUMEIKAN NTSOC LAB. 19

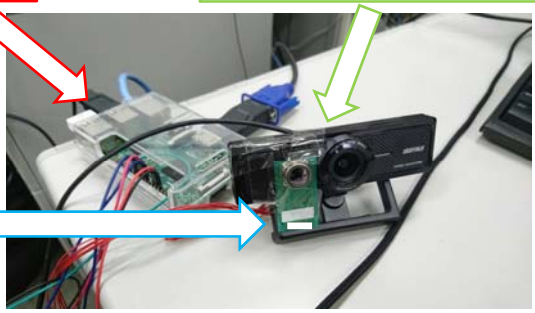
■ 低消費電力開発（チップ作製）からアプリケーションへ

組み込み機器に近い環境を想定

Raspberry Pi2 Model B
RAM: 1GB
CPU: ARM Cortex-A7 (4Core-900MHz)

iBuffalo製USBカメラ
BSW20KM11BK
USB接続,視野角120°（左右）
最大解像度1920*1080(Full HD)

赤外線アレイセンサ
SPI通信を用いて接続
視野角: 左右100° ・ 上下98°
16x16画素相当



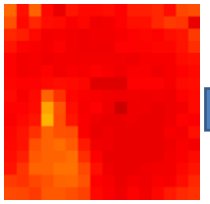
ソフトウェア処理環境:
主にC++言語を用いて実装
画像処理にOpenCV2.4を使用

顔検出処理にはHaar-Like特徴量を用いた
分類器(OpenCVに付属)を使用

（4）ラズパイ版GSSE監視カメラ応用

RITSUMEIKAN NTSOC LAB. 20

■ 赤外線カメラデータを利用してプライバシー保護領域を高速検出



赤外線アレイセンサの
温度情報

あるしきい値
温度で2値化

可視光画像と重ね合わせて
該当部分にのみ物体検出を適用

この領域は探索しない
↓
写真が検出されない

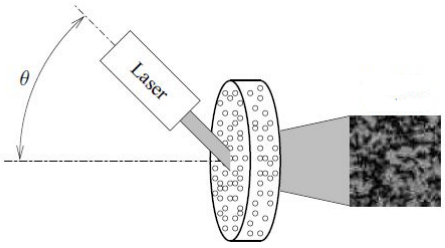
赤外線アレイセンサの温度情報から
物体検出の探索領域を制限することで
写真やマネキンなどの除去が可能

探索範囲

（5）PUF（Physically Unclonable Function）とは？

RITSUMEIKAN NTSOC LAB.21

- 人工物メトリックスによる真贋判定：人の指紋のように紙の模様・磁気体の磁力ムラなど人工物の偶然にできるパターンを活用
- LSIにおいてもトランジスタや配線の製造時のばらつきを利用し，ハードウェアの個体を判別する技術PUF（Physically Unclonable Function ）の研究が開始．
  ⇒LSIプロセスを使用したPUF（シリコンPUF）



Optical PUF [1]

Coating PUF [2]

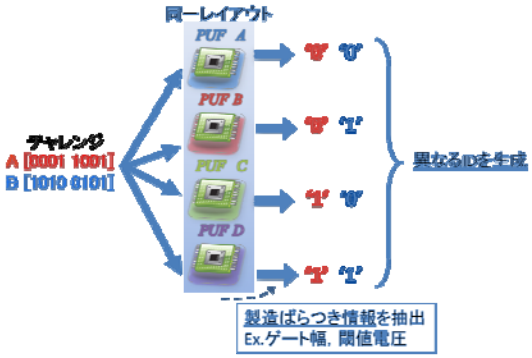
[1] Blaise L.P.Gassend, “Physical Random Functions”, MIT 2003
[2] Pim Tuyls, Geert-Jan Schrijen, Boris Skoric,Jan van Geloven, Nynke Verhaegh, Rob Wolters,“Read-Proof Hardware from Protective Coatings”, CHES 2006, p369- 383., 2006

（5）シリコンPUFの動作原理

RITSUMEIKAN NTSOC LAB.22

トランジスタサイズ,閾値電圧,etc…

デバイスの製造ばらつきを抽出しIDとして変換
→偽造不可能なデバイス固有のIDを生成する



・デバイス固有
・人工的に制御不可能

1.チャレンジを入力する

2.製造ばらつきを抽出し
レスポンス(出力)に変換する

3.レスポンス列を生成し,デバイス固有のIDとする

チャレンジに対するレスポンスのペア(CRP)の正誤で認証

（5）PUFの車載セキュリティ応用

RITSUMEIKAN NTSOC LAB. 23

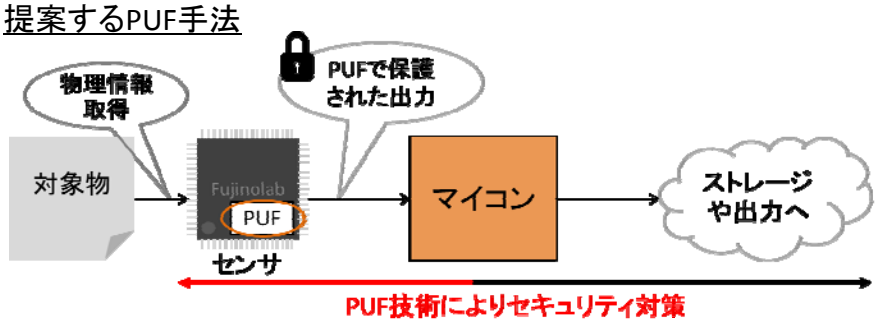
■ 鍵データをPUF IDで暗号化することで安全性を高める

（5）センサーへのPUF搭載

RITSUMEIKAN NTSOC LAB.

CMOSイメージセンサ自身の製造ばらつきをPUF技術に応用し，捏造されない画像を得ることを最終目的としている

提案するPUF手法

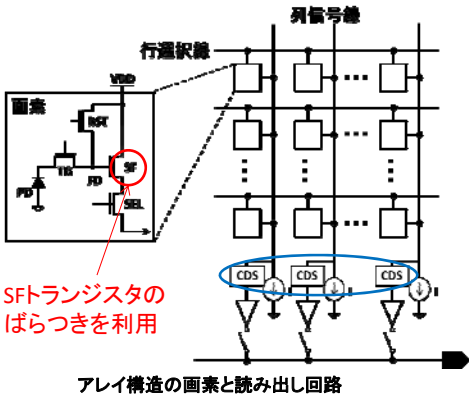


- 従来PUFに応用する時にはマイコンで処理を行っていた
- センサーマイコン間のセキュリティは未対策であり，不正アクセスなどによる情報の読み取りや改竄の危険性
- センサ内部に直接ばらつきを抽出する回路を搭載することによりPUF技術に応用する

（5）CMOSイメージセンサPUF

RITSUMEIKAN NTSOC LAB.

■CMOSイメージセンサと製造ばらつき



アレイ構造の画素と読み出し回路

画素の構成

PD：フォトダイオード
RST：リセットトランジスタ
TG：転送トランジスタ
SF：ソースフォロアトランジスタ
SEL：画素選択トランジスタ
FD：浮遊拡散層

CMOSイメージセンサのばらつき

固定パターンノイズ	ランダムノイズ
SFアンプのばらつき FD容量のばらつき PD特性のばらつき	リセットノイズ (kTCノイズ) ショットノイズ

ばらつき除去

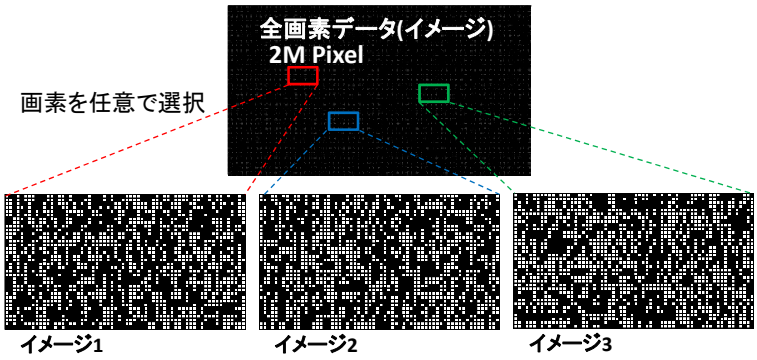
相関二重サンプリング（CDS:Correlated Double Sampling）と呼ばれる技術を用いてリセット信号電圧と画素信号電圧をサンプリングし，差分を出力することでばらつきを除去

（5）CMOSイメージセンサPUF

RITSUMEIKAN NTSOC LAB.

■実測データを用いたPUFのイメージ

シミュレーションと同じ画素数を任意で選択し，3つの画像を作成



表：各イメージ画像のHW

	1	2	3
HW	1181	1143	1104

表：各イメージ画像とのHD

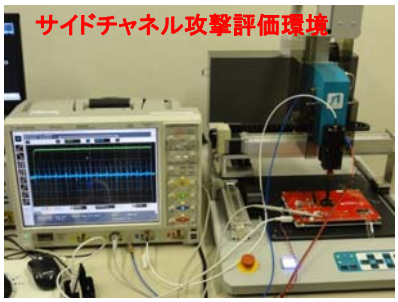
	1と2	1と3	2と3
HD	1181	1165	1101

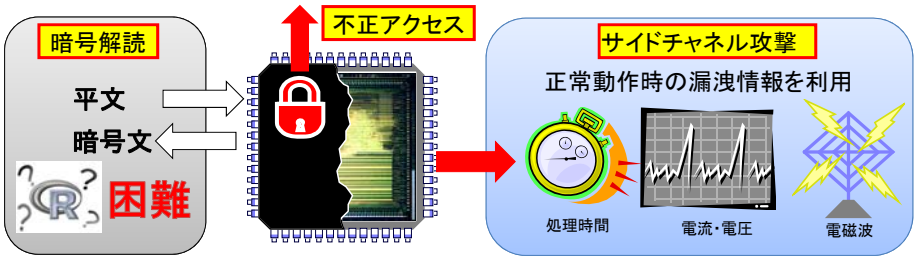
‘1’と’0’が偏りなく発生し，デバイスごとにユニークに出力している

（6）サイドチャネル攻撃（SCA）

RITSUMEIKAN NTSOC LAB. 27

- 暗号通信は万能ではない，鍵データが窃取されれば無効化される
  - ECUの鍵データ保管領域へのデバッグモードなどを利用した不正アクセスで鍵データを窃取可能
  - 車載ECUでも暗号回路動作時の電力や電磁波を用いて鍵データを窃取可能（サイドチャネル攻撃）



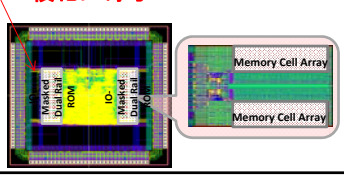


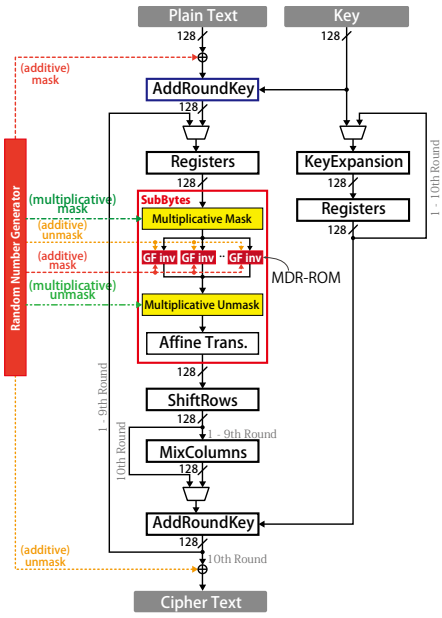
（6）SCAに耐性のあるAES暗号回路

RITSUMEIKAN NTSOC LAB. 28

- Sbox部に使われているメモリ部において乗算マスクを適用
- 乗算マスクにより，同一論理アドレスにアクセスしても，実際の物理アドレスはランダム化
- Sboxテーブルにはガロア体の逆元演算結果を格納する．これにより，暗号化と復号化でテーブルを共用化することが可能

Sbox用のメモリを半減することができ，小面積化に寄与

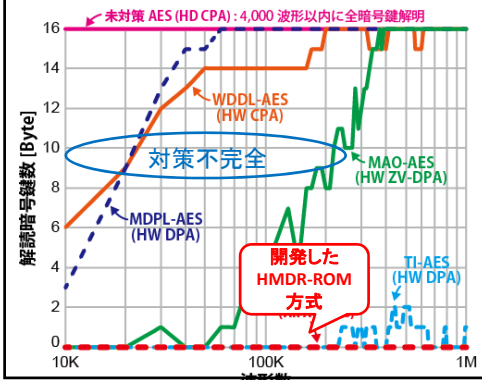


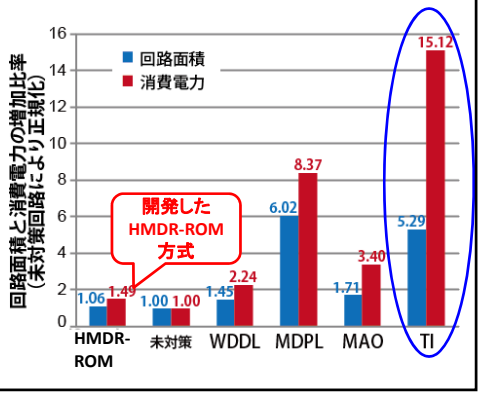


(6)HMDR-ROM方式の他の対策方式との比較

RITSUMEIKAN NTSOC LAB. 29

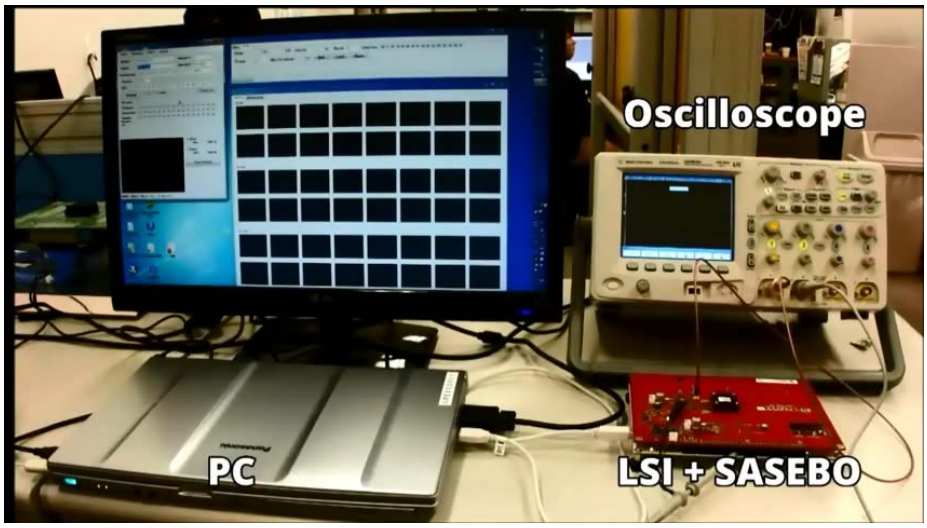
- 従来提案されてきた耐タンパ設計方式(WDDL,MDPL,MAO,TI)と比較して，耐タンパ性の検証およびチップ面積・消費電力を行った
- 耐タンパ性の評価は，産総研開発のSASEBO-RIIボードと定評あるオランダRicure社のソフトウエアを使用しEM攻撃の耐性評価も含めて各種の攻撃を実施(HW/HD-DPA, HW/HD-CPA, HW/HD-DEMA, HW/HD-CEMA, MIA)
- TI方式と提案方式は，100万波形でも1バイト以下のリーク，提案方式はTI方式と比較すると，面積1/5，消費電力1/10





MDR-ROM方式対策回路に対する電力解析攻撃実験デモ

RITSUMEIKAN NTSOC LAB. 30



現在行っている様々な研究

RITSUMEIKAN NTSOC LAB. 31

- 以下を簡単に説明しました.
  - (1) 実車ハッキング実験
  - (2) ソナーセンサへの攻撃基礎実験
  - (3) 赤外線と可視光画像の比較
  - (4) ラズパイ版GSSE監視カメラ
  - (5) CMOSイメージセンサPUF
  - (6)サイドチャネル攻撃
- 詳しく知りたい学生さんは，後のスライドに出てくる研究室訪問・見学の時間を活用してください.

卒論までのながれ

RITSUMEIKAN NTSOC LAB.

応用演習	2016/12-2017/1	・Raspberry Piのセットアップ ・Raspberry Piを使ったプログラミング実習 ・研究紹介（合宿＠エポック12/19予定）
輪講ゼミ	2017/2-2017/1	週1回「Understanding Cryptography」を読み進めます
春季演習 （週1回）	2017/2-3	Raspberry Piを使った班別プロジェクトの実施
院生ゼミ演習 （週2回）	2017/4-6	・LSI設計ツール（回路図，レイアウト，SPICE＆論理シミュレーション，論理合成）修得 ・FPGAおよびマイコンボード演習
卒業論文 テーマ選定	2017/4-7	院進学者は4月から研究準備開始 6～7月に最終決定（B4学生発表） 夏休みから本格研究開始
卒論目次作成	2017/12	卒論作成前に内容を整理,中間発表
卒論提出	2018/2	卒論提出

休み（ゼミの無い間）は，3月下旬（春休み）に2～3週間，8，9月に約1か月あります.

大学院について

RITSUMEIKAN NTSOC LAB.

- 研究の主体は大学院生
  - 4回生で学んだ研究のやり方を活用して，自主的に研究を進める能力を育成する．
- 学会発表
  - 国内学会（M1,M2）
    春（5月）「システムLSIワークショップ」
    冬（1月）「暗号と情報セキュリティーシンポジウム」
  - M2は海外発表・論文誌投稿が目標
    ISCAS，NCSP，SASIMI　など
- 対外研究交流
  - 耐タンパLSI設計,PUF：産総研，名城大，三菱電機，パナソニック
  - 赤外線センサ：機械工学科木股研究室，大阪産業大学
  - 車載セキュリティ：ヴィッツ，産総研，名古屋大学，スズキ，アイシン，三菱電機，ルネサスエレクトロニクス
- 過年度（2006-2016）の修士の就職先（含内定）
  - 東芝9，ローム4，日立4，富士通3，村田製作所2，デンソー3　ルネサスエレクトロニクス2，アドビックス2，NTT西日本2，富士重工2　他
  - 前までは半導体，最近は自動車関連が多い

研究室訪問・見学

RITSUMEIKAN NTSOC LAB.

- 個別相談は以下にメールでアポイントお願いします
  > fujino@se.ritsumei.ac.jp
- 配属希望調査前（詳細はHPで確認してください）
  - 10/31(月) 18:00頃～19:00頃（研究室説明会終了後）
    研究室見学＆教員面談＠藤野1研（ローム3F）
    研究室の研究内容＆設備を，デモ＆パネル展示で紹介します．
  - 11/1(火) 18:00～19:00
    院生による研究紹介＠藤野1研（ローム3F）
    院生・4回生が下記の内容に関して技術発表＆デモ展示を行う予定です．
    (1)車載セキュリティ技術
    (2)PUF(Physical Unclonable FUnctions)技術
    (3)サイドチャネル攻撃技術
    (4)赤外線アレイ併用低消費電力監視カメラGSSE

終わりに

RITSUMEIKAN NTSOC LAB.

- セキュリティに関する人材のニーズはますます高まっています．
  - モノがなんでもつながるIoTの時代には広範な領域で人材が求められています（コンピュータ・通信だけでなく自動車・インフラも）
- セキュリティ人材に求められる知識
  - ネットワーク技術・コンピュータ技術
  - 暗号技術（守るためには必須になる）
  - LSI（サイドチャネル攻撃やPUF技術）
  - センサー技術（IoTの末端神経はセンサー）
- しっかり研究室で活動して，社会で活躍できる人材に！

日本経済新聞

車・鉄道・飛行機を守れ　激化するサイバー交通戦争

2016/2/15 6:30 | 日本経済新聞　電子版

東京五輪が開かれる2020年に向けて、新しい交通インフラや法律の準備が着々と進むが、喜んでばかりもいられない。企業や政府機関に対するサイバー攻撃だけでなく、コンピューター制御が進んだ交通インフラもターゲットになる。自動車、鉄道、飛行機――。安全運転・運行（運航）をつかさどるそれぞれの現場では、目に見えぬ敵との戦いが始まった。

RITSUMEIKAN NTSOC LAB.