

電子情報工学科 藤野 毅・熊木 武志
応用演習研究室紹介 2014.10.6

ネットワークLSIシステム研究室 (Network System On Chip Lab.)

1

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
- 研究室メンバー
 - 教授：藤野 毅
 - 講師：熊木 武志（小倉研と兼任）
 - 研究員：汐崎 充， 久保田貴也
 - 研究補助員：浅川 俊介， 清水 明恵（秘書）
 - 客員研究員：熊本 敏夫（大阪産業大学）
 - (D3)1名， (M2)：8名， (M1)：4名
 - 学部学生(B4)：9名（5名がM1に進学予定）

2

研究室でやりたいこと

(1)自動運転へ向けた安全な自動車

- 赤外線カメラで夜間も安全
- インターネットとの通信
- 安全な車-車通信，車-人通信
- 車載ソフトウェアの安全なアップデート

(2)ビッグデータ時代のセンサーノード

- 画像のプライバシーが保護
- 農場など電源がなくてもデータ収集可能
- 赤外線センサーを使ったノーマリオフ動作で低消費電力化（専用制御ハードウェアとアナログ回路）
- 赤外線センサーの自動車応用や介護応用を視野に

(3)偽物・犯罪の被害を防止する

- 電子すかし・改ざん防止・盗撮防止
- ハードウェアトロイ検出
- 耐リバースエンジニアリング

研究プロジェクト

(1)自動運転へ向けた安全な自動車

- CREST 耐タンパVLSI(～2015/3)，IPA (～2016/3+)
 - M2 中井，西村，竹内，堤，M1 北村
- enPIT (～2016/3) 車載セキュリティー（名古屋大学）
 - M1 中野（with 富山研究室，名城大学）
- サポイン：車載ゲートウェイへのPUF応用(～2017/3)

(2)ビッグデータ時代のセンサーノード

- NEDO：ルネサス(～2016/3)ノーマリオフ
 - M2 中川
- STARC：(～2017/3)グリーンスマートセキュアアイズ
 - M2 人見，M2 柳原，M1 上口（with 木股研，大阪産業大学）

(3)偽物・犯罪の被害を防止する

- 科研費：ハードウェアトロイ・盗撮防止
 - M2 塚田，M1 蔭山

(1)自動運転へ向けた安全な自動車

- 赤外線カメラで夜間も安全
- インターネットとの通信
- 安全な車-車通信, 車-人通信
- 車載ソフトウェアの安全なアップデート

(2)ビッグデータ時代のセンサーノード

- 画像のプライバシーが保護
- 農場など電源がなくてもデータ収集可能
- 赤外線センサーを使ったノーマリオフ動作で低消費電力化 (専用制御ハードウェアとアナログ回路)
- 赤外線センサーの自動車応用や介護応用を視野に

(3)偽物・犯罪の被害を防止する

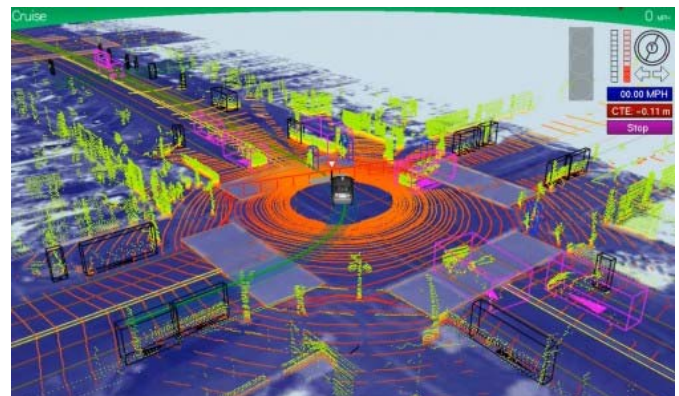
- 電子すかし・改ざん防止・盗撮防止
- ハードウェアトロイ検出
- 耐リバースエンジニアリング

(話題 1)グーグルの自動運転車

- 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

(話題2) ハッカーがプリウスをクラッキング

- 2013年夏のニュース（朝日新聞等でも掲載）
- 米ラスベガスで開催中のハッカーの祭典「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。IT化が進む車のセキュリティー強化に向け、注意を呼びかけた。
- 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
- <http://matome.naver.jp/odai/2138734632741391601>



7

自動運転車への進化

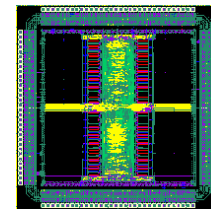
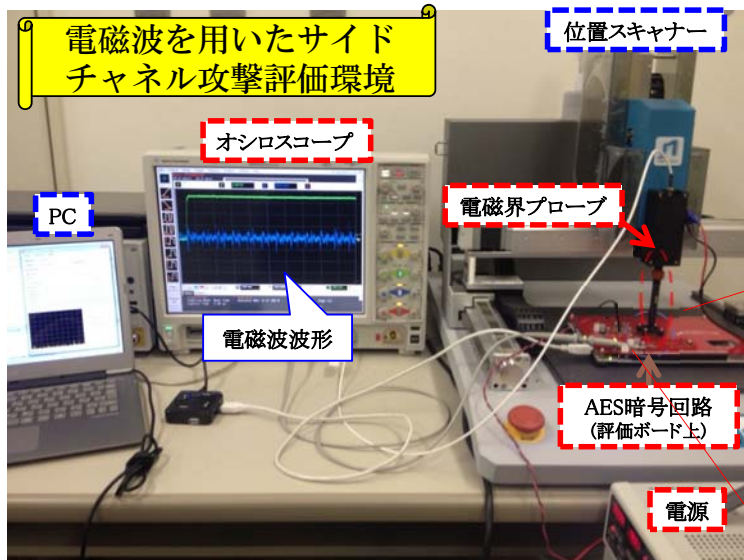
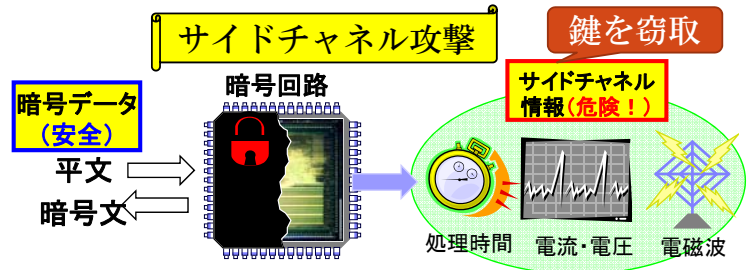
- 運転者の指示のみに基づいて制御されていた自動車が、
 - 1) 自動車に搭載されているセンサ（レーダー・カメラ）で制御
 - 2) インターネット回線等の外界の情報
 で制御されていく



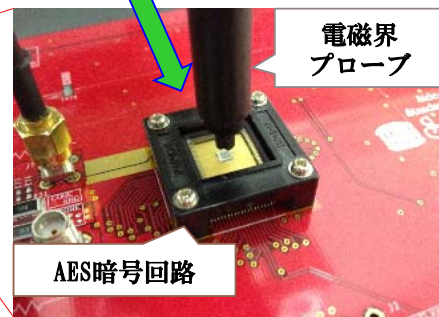
8

【技術】耐タンパAES暗号回路

- 暗号回路が動作しているときの、消費電力や電磁波を利用して、暗号鍵情報を窃取する「サイドチャネル攻撃」に対して耐性のある回路を開発。



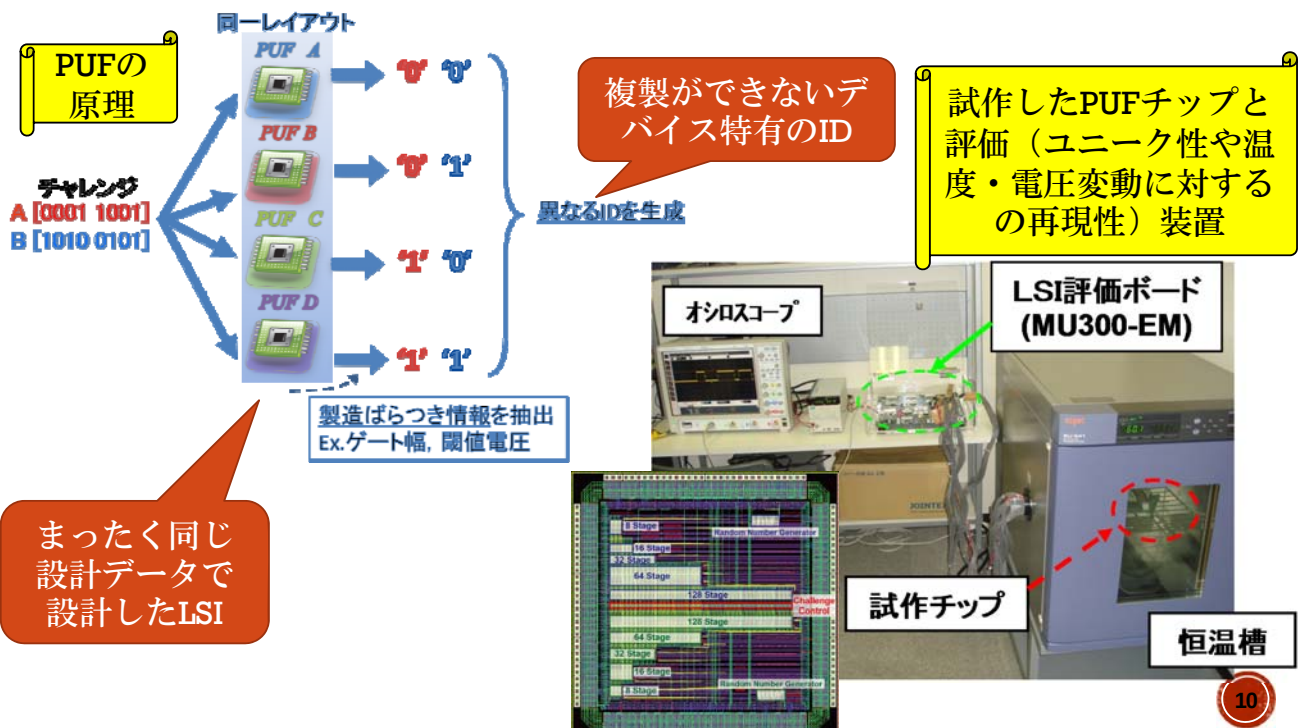
設計した耐タンパ
AES暗号回路
(ローム0.18μm
CMOS)



9

【技術】PUF技術

- LSIの製造時のばらつきを使用して、固有のIDを発生する技術 (人間で言えば指紋やDNAのようなもの)
- 模造品防止やICカードには実用化が始まりつつあるが車載応用を検討中

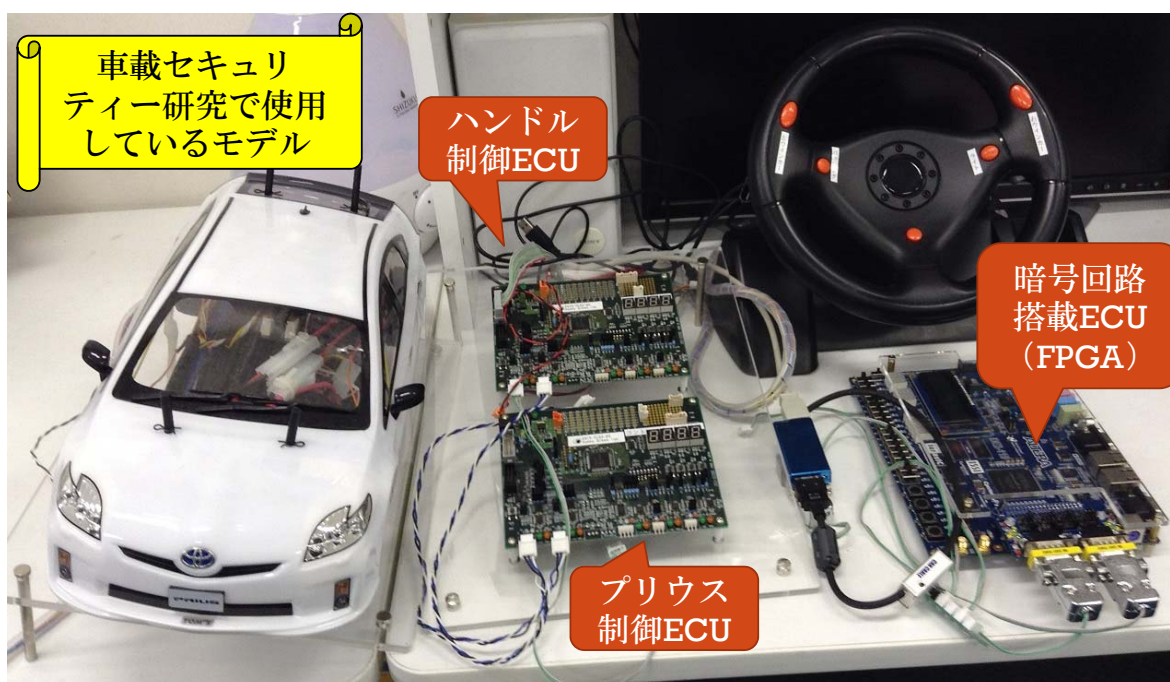


10



車載LANセキュリティの研究

- 現状の車載LAN(CAN通信)は、暗号や認証をまったく行っていないので、侵入して外部制御を行うことが可能
- 暗号回路とPUFを実装し、AUTOSAR（次世代車載OS）上で、CAN通信を暗号化または認証付通信に変更することで、車載制御のつとりを防止する



研究室でやりたいこと

(1)自動運転へ向けた安全な自動車

- 赤外線カメラで夜間も安全
- インターネットとの通信
- 安全な車-車通信, 車-人通信
- 車載ソフトウェアの安全なアップデート

(2)ビッグデータ時代のセンサーノード

- 画像のプライバシーが保護
- 農場など電源がなくてもデータ収集可能
- 赤外線センサーを使ったノーマリオフ動作で低消費電力化 (専用制御ハードウェアとアナログ回路)
- 赤外線センサーの自動車応用や介護応用を視野に

(3)偽物・犯罪の被害を防止する

- 電子すかし・改ざん防止・盗撮防止
- ハードウェアトロイ検出
- 耐リバースエンジニアリング

13

(話題3) 「ビッグデータ」

- NHKクロースアップ現代 (2012.5.28)
「社会を変える“ビッグデータ”革命」
- NHKスペシャル (2013.3.3)
「“いのちの記録”を未来へ ～震災ビッグデータ～」
- ニュース深読み (2013.6.22)
「“ビッグデータ”で暮らしはどう変わる？」

政府が成長戦略の柱として注目する“ビッグデータ”。

ネットやカメラ、センサーなどによって、今や私たちの生活が“データ”として収集できる時代に…。その膨大な情報 (= ビッグデータ) を活用すれば、第二の産業革命に匹敵する経済効果があるともいわれています。

国や企業が積極的にビッグデータ活用を推進したら、私たちの暮らしや経済はどう変わるのか？ 情報の安全面は？

街中のいたるところに監視カメラが設置され、行動を把握されている。



現在の監視カメラの問題点

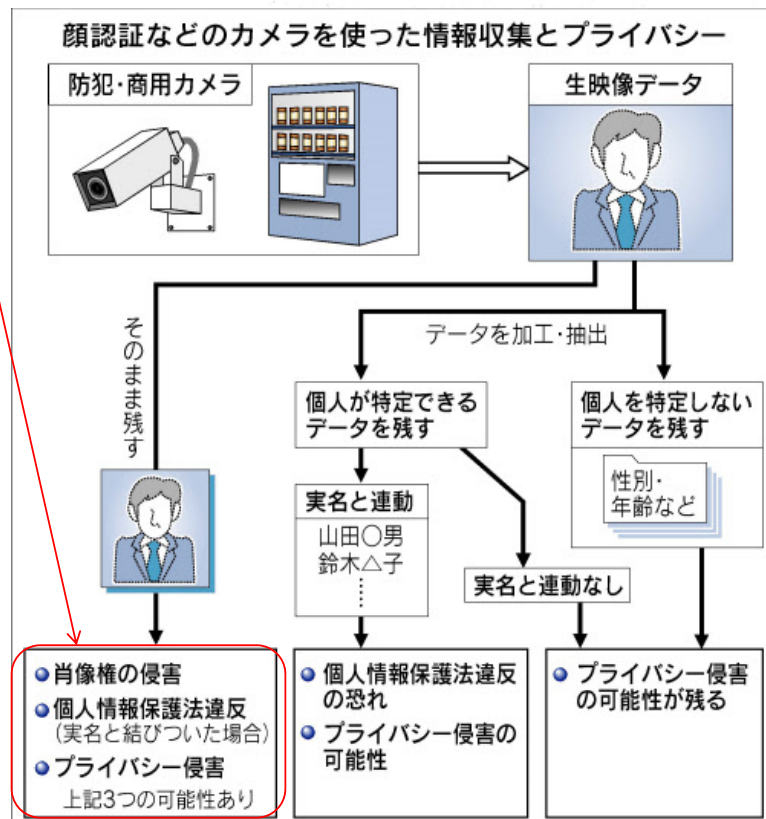
(1) プライバシー保護

生画像データをそのまま保存すると肖像権の侵害・個人情報保護法違反・プライバシー侵害の可能性

(2) 夜間の監視

(3) 監視ネットワークへのサイバー攻撃

(4) 低消費電力化



【技術】画像プライバシー保護技術

- カメラ取得画像から自動で顔を検出して、暗号技術を用いた階層型部分画像マスク (HMF) を印加する。
- 事件・事故等が生じた場合には、権限者が秘密鍵を用いて元画像を復元できる
- 低消費電力基板を用いたデモシステム構築
 - 組み込みシステム技術展ET-West2013 (インテックス大阪) で技術展示を行い好評
- 今後の研究課題
 - 顔検出の高速化
 - 動画フォーマットへの対応



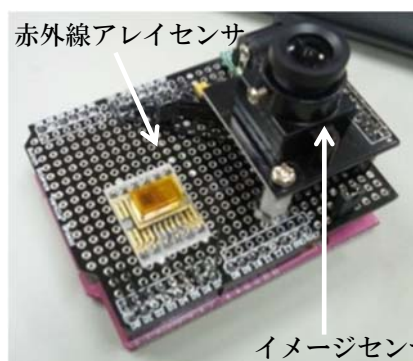
【技術】夜間の監視：赤外線センサ

- 夜間の監視・可視光では検知できない機器不良監視が可能
- 起電力型（サーモパイル）センサは原理的には低消費電力

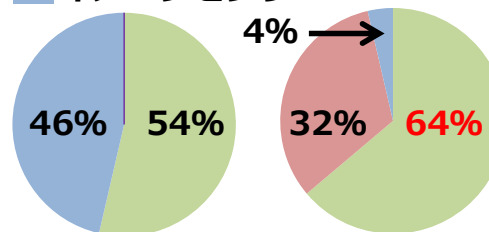


【技術】ノーマリオフ制御技術

CMOSイメージセンサと赤外線アレイセンサを組み合わせ、マイコンで制御。間歇動作で低消費電力化。



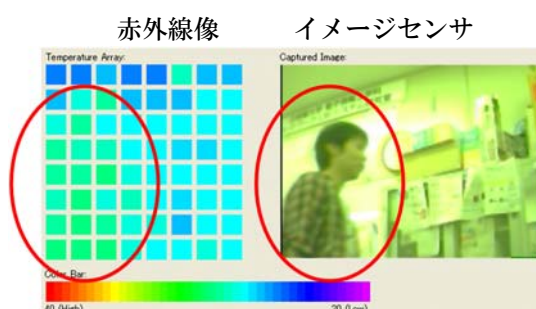
■ マイコン ■ IRアレイセンサ
■ イメージセンサ



N-off262mW

N-off11mW

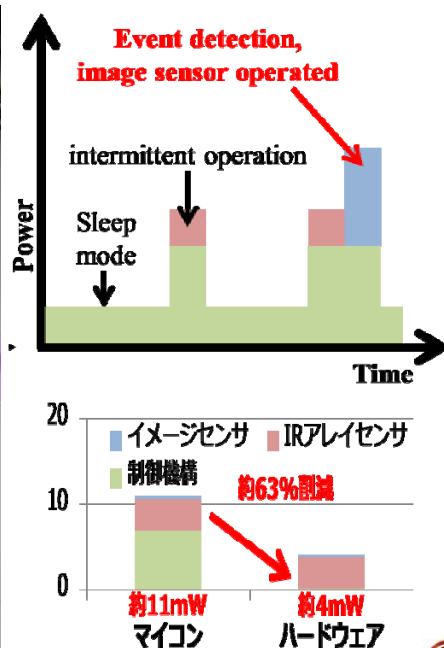
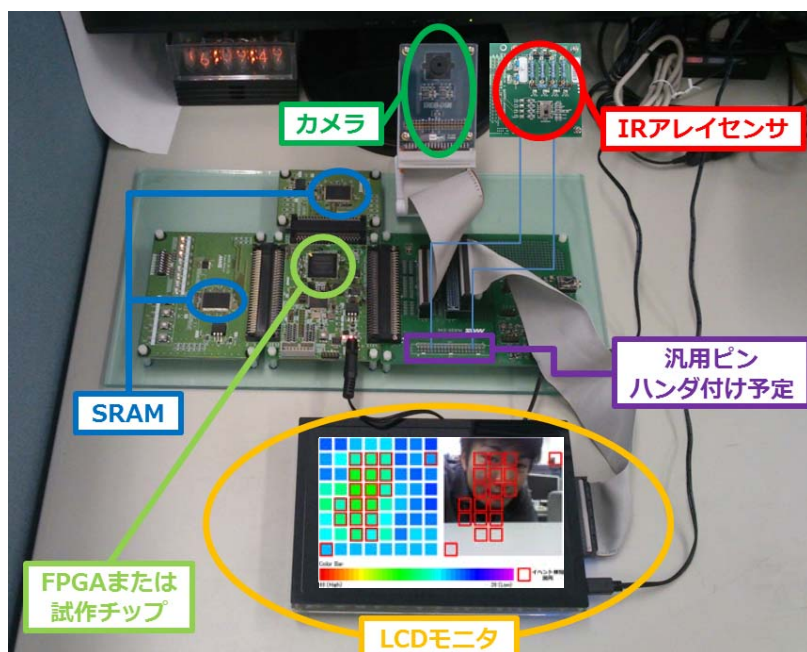
シナリオ：1s毎赤外線センサ起動，60s毎画像取得



- さらなる低消費電力化のために
- (1) マイコン(MCU)の動作をハードウェアシーケンサを用いて実現
 - (2) 赤外線(IR)アレイセンサのアナログフロントエンド回路の低消費電力化

GSSEデモ機(開発中)のイメージ

間歇動作を行うマイコンの制御をハードウェア化する
FPGAボードを用いてデモンストレーション機開発中



19

GSSE技術で社会に安全と安心を



20

赤外線センサを用いた人物検知技術 ～車載センサー＆介護応用への展開～

- 赤外線アレイセンサは夜間の監視が可能
 - 自動車の安全
- 夜間に人物を監視でき、かつプライバシー侵害も少ない
 - 人物動作検知による介護応用



Autoliv (赤外線カメラで夜間走行アシスト)



21

研究室でやりたいこと

(1) 自動運転へ向けた安全な自動車

- 赤外線カメラで夜間も安全
- インターネットとの通信
- 安全な車-車通信, 車-人通信
- 車載ソフトウェアの安全なアップデート

(2) ビッグデータ時代のセンサーノード

- 画像のプライバシーが保護
- 農場など電源がなくてもデータ収集可能
- 赤外線センサーを使ったノーマリオフ動作で低消費電力化 (専用制御ハードウェアとアナログ回路)
- 赤外線センサーの自動車応用や介護応用を視野に

(3) 偽物・犯罪の被害を防止する

- 電子すかし・改ざん防止・盗撮防止
- ハードウェアトロイ検出
- 耐リバースエンジニアリング

22

(話題3) 偽物の横行

- 半導体の模造品が大きな問題となっている
 - 模造品発見数は年々増加
 - 半導体の模造品市場は世界の半導体市場の5%
- セキュリティ用ICチップも秘密情報を盗むことで複製可能
- まだ単なる、模造品ならマシで、中には、悪事を働く模造品（ハードウェアトロイ）も

⇒次スライド

特集

その電子部品 ホンモノですか?



巷にあふれる模造電子部品	p.30
第1部: 模造 部品供給の穴を突き、機器の安全を脅かす 中国ではびこる模造自動車部品	p.32 p.41
第2部: 知能 チップに固有のIDを付与、国際標準を巡り各国が火花	p.44

(取材協力: Phil Keys, 内田 肇)

*日経エレクトロニクス,
2010/4/19号

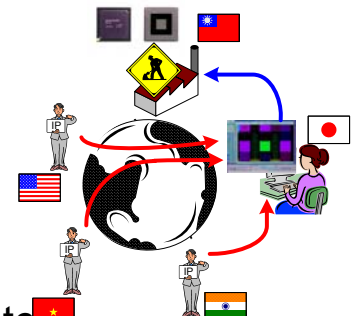
23

ハードウェアトロイの恐ろしさ

狙われる半導体LSI

- 不特定多数の人がLSI開発に関わる。
 - 世界で集積回路の設計を手掛ける企業数: 約1,550社
 - 半導体LSIの年間設計数: 約2,500個
 - 世界の半導体売上高 (2009年): 約\$2,350億
 - グローバル化に伴い、LSI本体の設計やそれに用いるハードウェア・ソフトウェアIPの製作に関わる人々は世界規模で数百人、数千人規模。
- 微細化に伴うLSIの多機能化がハードウェアトロイを生んだ。
 - 設計者に対して性善説を前提として良いか。
 - 設計データがハッキングされたら。
 - LSI機能ブロックや、IPにハードウェアトロイが仕込まれ世界中に利用される: ASIC, FPGA, etc...
 - いったい何が起るのか?

耐震偽装,
牛肉偽装...



24

ハードウェアトロイによる被害例

軍事装備品が狙われた可能性がある

- 軍事作成の成功の裏に
 - イスラエルがシリアの施設を攻撃した際，イスラエル空軍は、シリアに気づかれることなくレーダー（ロシア製）網をくぐり抜け，目標を破壊して無傷で帰還．
 - シリアのレーダーを構成する部品であるマイクロチップに，あらかじめ，バックドアが仕込まれていた！
- ハードウェアトロイに対する日本の状況.
 - 関連研究発表は殆ど行われていない．
 - 半導体関連企業も，未だ対策を行っていない？
 - 立命館大学でこの分野の先駆者を目指す！

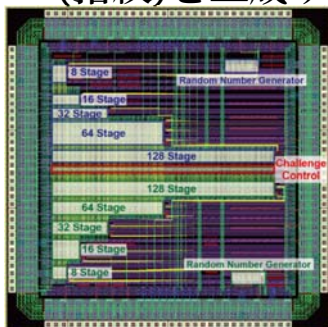
我が国においても早急な対策が必要
となってきている！



25

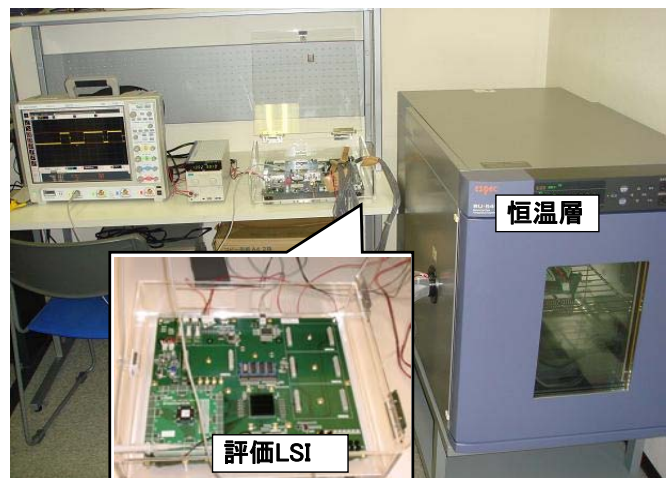
(3-1) LSIを模倣させないために

- PUF（Physical Unclonable Function）技術
 - LSI製造時のトランジスタのばらつきを利用してそのチップ固有のID(指紋)を生成する



試作PUFチップ

温度や電源電圧が変動しても同じID
が生成されるかをテストする ⇒



- 耐リバースエンジニアリング技術
 - LSIのレイアウトを解析（リバースエンジニアリング）して，まったく同じ商品を作ってしまう被害
 - 容易にレイアウトを解析させないLSI設計技術：Diffusion Programmable Logic(DPL)

26

(3-2) 画像の構造解析に基づく改ざん検出

デジタル画像データは，こんな特徴があります．

0101011001010101...

- ◎ 誰でも取り扱いが容易．
- ◎ コストを削減できる．
- ◎ パソコンやスマホで加工編集が可能．

そのデジタルデータ，改ざん
されていませんか？？

デジタル画像が使える？？
法廷，工事現場，証拠写真，etc



27

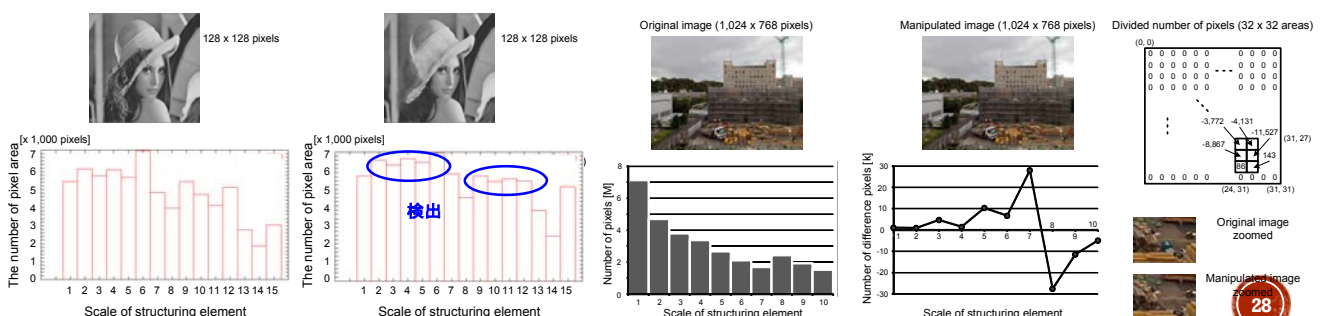
デジタル画像に信頼性を与えるには

デジタル画像内の特徴をパターン化，暗号処理によってパターンを
秘匿し，オリジナル性を保証．

- ◎ 画質の低下無し．
- ◎ 元データの必要無し．
- ◎ 数ビットの改ざんも検出可．
- ◎ 改ざん位置も判明．
- ◎ ノイズ耐性も有り．

モルフォロジカルパターンスpektrumと
公開鍵暗号を利用

使っちゃオ！
信頼しちゃオ！



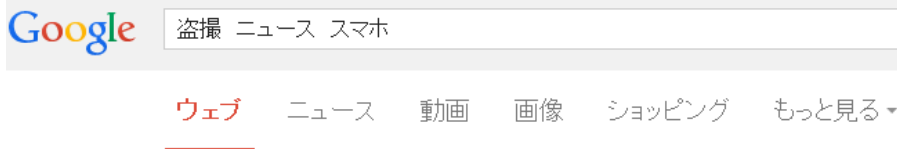
28

(3-3) LED照明とスマホカメラの連携による盗撮防止システムの開発

スマートフォンの普及による手軽さが災いして...

これは... どちら？

- ・ キーワード: 盗撮 ニュース スマホ



約 5,860,000 件 (0.20 秒)

浴室窓からスルッとスマホ 神奈川県警警部が盗撮疑い - MSN ...
sankei.jp.msn.com/affairs/news/140813/crm14081300350003-n1.htm

- (2014.8.19) 勤務先トイレで女性を盗撮 福井
- (2014.8.13) 浴室窓から県警警部が盗撮 神奈川
- (2014.8.6) 防衛省幹部女性を盗撮 千葉
- (2014.7.24) 教室で盗撮高校生書類送検 京都
- (2014.7.31) 高校教諭, スカート内盗撮 秋田
- (2014.4.26) 地下鉄内で盗撮 大阪
- (2014.4.14) 新聞記者スーパーで盗撮 栃木 ...たくさん!



<http://www.akb48matomemory.com/archives/1005952156.html>

29

開発目標：可視光を利用した盗撮防止システム

可視光ビーコンを利用して, カメラに対し直接様々な制限をかける！

- ・ LED照明をマイコン制御しビーコン発生
- ・ カメラによる取得画像をソフト or ハードレベルで処理し, 機能制限



30

可視光を利用した盗撮防止プロトタイプシステム

実用化に向けての実験プラットフォーム

- ・ LEDシーリングライトをマイコン制御し
- ・ スマートフォンの撮影アプリを開発して機能制限

- ・ 2014.7.29～30: 組込み総合技術展関西 (ETWEST2014)出展
- ・ 2014.8.22: 京都産学公連携機構主催未来技術交流会で講演



31

藤野・熊木研究室
での研究生活とは？

32

研究成果発表の様子

・ 最近の学会

(国際) アメリカ, ハワイ, カナダ, トルコ, ブラジル, 台湾 etc.

(国内) 北海道, 福岡, 鳥取, 東京, 富山, 沖縄, 鹿児島 etc.

・ 論文誌にも掲載

・ 国, 企業等とのプロジェクトも進行中



FIT2011@函館

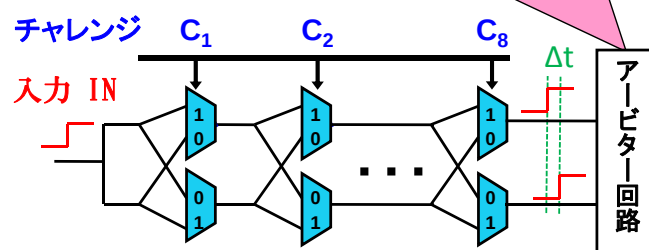
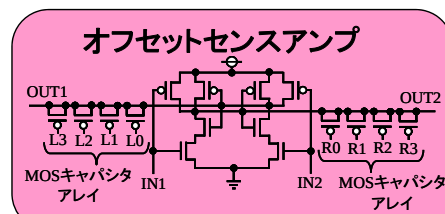
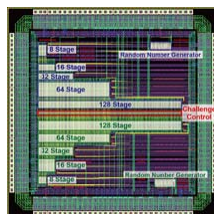


MWSCAS2013@アメリカ

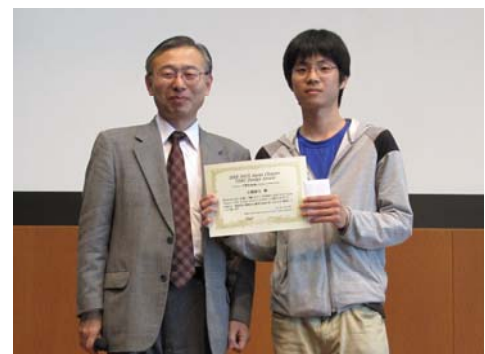
33

【表彰】 VDECデザインコンテストNO.1

- VDEC (東京大学大規模集積システム設計教育センター)
- 2011年に日本の大学で試作されたチップの中で当研究室M2の古橋君が「遅延時間差検出型アービターPUF」の研究で、最優秀賞を受賞しました
- 本研究は、ブラジルでの国際学会でも発表。



試作PUF回路(ローム0.18μmCMOS)



VDECセンター長
東京大学浅田教授

34

【ニュース報道】盗撮防止技術が紹介される

■ 京都大学記者クラブにて報道発表

○ニュース番組、グッド！モーニング、及びかんさい情報ネットtenで紹介される。

○日本経済新聞、読売新聞、産経新聞、朝日新新聞、産経新聞、毎日新聞、日刊工業新聞、京都新聞、中日新聞、NEWS立命。

○JSTサイエンスポータルニュース速報で紹介される。

○Yahoo!JAPANのニューストップ等で紹介される。



35

展示会にも積極的に出展



立命館大学 電子情報工学科 ネットワークLSIシステム研究室

<http://www.ritsumeikan.ac.jp/se/re/ec/index.html>

R RITSUMEIKAN

近年、監視カメラは犯罪捜査における犯人特定や証拠画像等の重要な情報源として利用されていますが、不特定多数の人物に対して撮影を行うため、個人情報保護の観点から配慮が必要となります。当研究室では映像中の顔情報等を検出し、要求に応じて強度や取り外しの制御が可能なマスク処理技術を紹介し、組み込み機器を利用した監視カメラ内で適用している様子を展示します。また、画像改ざん検知ソリューション等の技術も紹介します。

http://www.jasa.or.jp/etwest/2013/exhibitor/newlist_in.html



36

<https://www.starc.jp/events/workshop2013/>

卒論までのながれ

応用演習	2014/12-2014/1	・PC環境,Cygwin環境セットアップ ・Cプログラミングによる暗号回路 ・研究紹介(合宿@エポック12/22予定)
輪講ゼミ	2015/2-2016/1	週1回「Introduction to VLSI Circuits and Systems」を読み進めます
春季演習 (週1回)	2015/2-3	C言語の演習(簡単な暗号プログラム) 論理回路演習(SPICEシミュレーション)
院生ゼミ演習 (週2回)	2015/4-6	・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	2015/4-7	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	2015/12	卒論作成前に内容を整理, 中間発表
卒論提出	2016/2	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3~4週間あります。

37

大学院について

- 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」
 - 秋 (11月) 「デザインガイア」
 - 冬 (1月) 「暗号と情報セキュリティシンポジウム」
 - 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, デンソー
 - ノーマリオフセンサ: ルネサスエレクトロニクス, 大阪産業大学
 - 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 (2006-2013) の修士の就職先 (含内定)
 - 東芝9, ローム4, 日立4, 富士通2, 村田製作所2, デンソー2
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 他

38

先輩の成果（2013年修士中間発表会）

- 最優秀賞 人見君「センサーノードのノーマリオフと制御機構のハードウェア化による省電力化」
- 優秀賞 中井君「AES暗号回路にいける電磁波解析技術とリーク原因の検証」
竹内君「AES暗号回路とPUFの統合チップアーキテクチャの検討」



研究室訪問・見学

- 今週（アポイントメントなし，個人研究室）
 - 10/6（月） 18:00～19:00（このあとすぐ）
* 上記以外の個別相談はメールで予約してください
> 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）
 - 11/3(月) 17:00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。
 - 11/4(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)製造ばらつきを利用した固有ID生成技術
 - (2)耐タンパ暗号LSI設計
 - (3)超消費電力センサーネットワーク技術
 - (4)モバイル機器向けLSIとセキュリティ応用

終わりに

- 論理設計～回路設計～物理設計まで**LSI**設計の実践力を
 - 「自分で作製したチップが所望の動作をしたときは感動しました」と研究室の学生の声
 - 評価測定をすることでボードや測定機の扱い方をマスター
- **CPU**ボード・**FPGA**ボードを使ってシステムを作ろう
 - ソフト（車載**OS**）・ハードの総合的な理解ができる
 - 作成したシステムを使って展示会でアピール
- ネットワーク（セキュリティ）技術の知識を身につけよう
 - 暗号や乱数の知識は今後ますます重要に
- 歓迎する学生像
 - いろいろなことに好奇心があり興味を深める
 - 自分で考えて行動できる
 - 責任感を持ってコミュニケーションできる
- 研究室学生の**Wiki**（イントラネット）を見ると当研究室のアクティビティーの一端が感じられるでしょう！
⇒<http://rh5pt200.bkc.ritsumei.ac.jp/wiki/>