【ネットワークLSIシステム（藤野・熊木）研究室】

～医療・介護・自動車等において，安心・安全を実現するソフト＆ハードウエア～

○研究紹介

ネットワークLSIシステム研究室においては，「通信ネットワークにより相互に接続されたLSIシステム」に関連する研究を行っています．このようなシステムの代表としては，多数のマイコンがネットワークで接続された自動車（図１）や，社会や家庭で，省エネや安心・安全のために普及進むセンサーネットワーク（図２）などがあります．

図１．多数のコンピュータ・センサーから構成される自動車（車載ネットワーク）

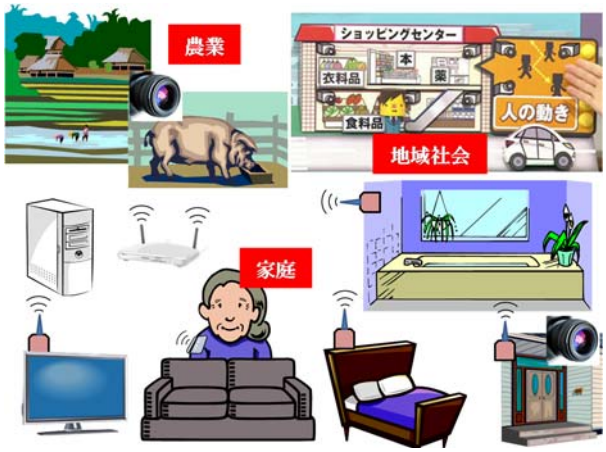


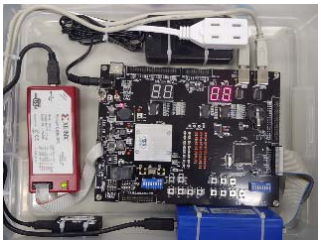
図２．家庭・地域社会・農業で普及するセンサーネットワーク

インターネットに接続される自動車やセンサーネットワークにおいては，セキュリティー・プライバシー確保のために暗号技術が用いられます．また，バッテリー駆動のセンサーでは低消費電力技術も欠かせません．当研究室は，2009年より開始した大型の国プロ「CREST」で開発し世界トップレベルの，悪意ある攻撃に耐性のある耐タンパ暗号LSIの設計技術を持っています．また，2012年より開始した国プロ「NEDO」研究の受託では，ノーマリオフ超低消費電力センサー技術の開発を行ってきました．また，今年から開始した「STARC」研究では，赤外線アレイセンサと可視光カメラをハイブリッド動作させる極低消費電力監視カメラ「スマートセキュアアイズ」のハードウエア＆ソフトウエア開発を始めました．これらのプロジェクトを，教員（藤野，熊木），研究員（汐崎，久保田），研究補助員（浅川）と大学院生13名（内博士課程１名），学部生９名が，他大学（名古屋大学・名城大学）や，産業技術総合研究所・IPA・ルネサスエレクトロニクス・三菱電機・デンソー・ヴィッツ等の産業界と交流しながら行っています．

【藤野・熊木研研究プロジェクト：複数のプロジェクトに参加する学生もいます】

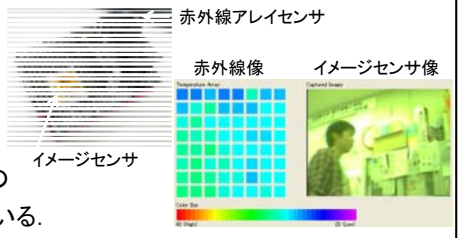
<MX> モバイル機器向けLSIとセキュリティ応用

モバイル機器向けLSIの開発とその応用を行っている．現在は暗号化，電子透かし，画像マスク法，改竄防止，盗撮防止及びハードウェアトロイ等について研究中．また，2,048超並列処理LSIや小型マイコンボードを用いたアプリケーション開発も行っている．



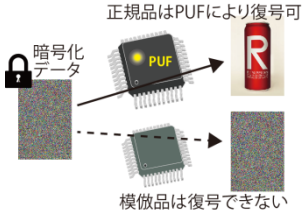
<SN> 超低消費電力センサーネットワーク技術

乾電池で数年稼働する超低消費電力センサノードの開発とその応用を行っている．現在は温度や湿度のセンサー特性を検証して，基板を開発するとともに，赤外線センサやイメージセンサを組み合わせたイベント起動型の防犯装置を開発している．



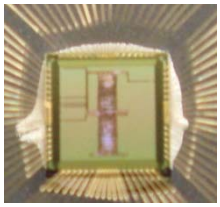
<PUF> 製造ばらつきを使用した固有ID生成技術

最近，話題となったiPhone向け模造品充電器による感電事故のように模造品の製造・販売による被害を多くの企業が経験しており，年々被害が拡大している．当研究室では模造品防止技術として，LSIの製造ばらつきからデバイス毎に固有IDを持たせるPhysically Unclonable Function (PUF)技術の開発を行っている．



<SCA> 耐タンパ暗号LSI設計

暗号回路は，ICOCAなどの電子マネーなどに使用されているが，動作時の消費電力や電磁波をモニタすることで暗号鍵を推定するサイドチャネル攻撃が脅威となっている．これらの攻撃から暗号回路を守る設計技術が「耐タンパ設計」であり，当研究室オリジナルの2線式RSLメモリを用いたDESおよびAES暗号回路を設計し耐タンパ性を評価している．



○使う研究設備

当研究室のポリシーは，**モノを作って評価する**というところです．マイコンや FPGA ボードを使ったシステムはもちろんのこと，LSI の設計・評価も行っています．マイコンボードでは，携帯電話等にも使用されている低消費電力 ARM マイコンを用いて，図３に示すようなプライバシー保護監視カメラを構築して，2013 年 6 月には組み込みシステム展でデモンストレーションを行いました．企業からも注目され，医療・介護で見守り等の用途への応用を期待されています．暗号 LSI 設計では，暗号回路の鍵を LSI 動作時の消費電力や，漏えい電磁波を使って不法に窃取するサイドチャネル攻撃への対策が必要となっています．このような攻撃への対策を行った暗号 LSI を実際に試作し，図４に示すような実験装置を用いて，電磁波を使った攻撃を実際に行い，暗号 LSI の安全性を評価しました．本研究の成果を使って，車載 LAN やセンサーネットワークにおける不正アクセス防止に向けた研究もしています．

研究を進めるうえで，マイコンや FPGA ボード実装，LSI 設計を行い，様々な評価を行うことを通して，工学部の原点であるモノづくりの面白さ・重要性を体験するとともに，社会人になってから必要な，C(C#)，verilogHDL，MATLAB，電子回路，アナログ回路に関する実践的な技術を身につけていくことができます．

図３．プライバシー保護監視カメラシステム

図４．電磁波を用いたサイドチャネル攻撃実験設備

○卒業研究の進め方・大学院での研究

応用演習が終了する２月中旬以降，週１回教員が指導する LSI の英文書の輪講と LSI 設計に関する簡単な演習が始まります．４月に入ると，上記に加え，ネットワークに関するゼミ輪講をおこなうほか，大学院生から C や verilog HDL のプログラミングと FPGA 実装および SPICE シミュレータなどのツール実習を週２回程度受け，卒業研究に必要な知識を修得していきます．**院進学希望学生は，並行して，４回生の４月に仮研究テーマを選択して，院生と一緒に研究を開始**します．４回生の夏頃，卒研での研究テーマを最終決定して本格的に卒業研究を開始します．

大学院に関してですが，研究および技術開発職に就きたいのであれば進学を勧めます．修士課程で，学会発表や企業との共同研究の打ち合わせに参加することで，**企業で実際に求められている技術スキルの内容やレベルを実際に感じて，自分の能力をどのような企業のどんな分野で活用したいのかが分かってくる**と思います．

当研究室では国内学会・国際学会などに積極的に参加してもらっており，この３年間は，毎年国内学会に 20 件以上，国際学会 5 件以上を発表しています．2011 年 5 月には，全国の大学・高専で設計・試作された LSI の年間 No.1 を決定するコンテストで，当研究室の M2 が，最優秀賞を受賞しました．また，2012 年 9 月には，電子透かし技術の統一評価基準を定める世界初のコンテストで技術が認定されました．さらに，2013 年 3 月および 2014 年 3 月と 2 年連続ハワイで行われた学会で当研究室の M2 が表彰されています．皆さんも，日本のトップレベルの研究を行って，その技術を世界にアピールしていきましょう．**学会発表等で得られた，論理的思考力とプレゼンテーション能力**は，就職活動でも非常に有益で，学会発表でがんばった学生ほど，早く希望の会社から内定を得られるという傾向があります．

○さいごに

・資源のない日本が今後も繁栄していくためには，やはり高い技術力を持ち続けることが一番大事だと考えています．それを担っていく技術者の卵である皆さんには，**学生時代には，技術スキルだけでなく，新しい技術に対する好奇心を持って欲しい**と思います．新しい技術分野で，自分のアイデアとそれを実現する技術を持ち，それを他の人に広めるプレゼンテーション能力を身に着けて，日進月歩の電子情報技術分野で長く活躍できる力をつけてください．

・そのための環境をこの研究室では用意していきたいと考えていますので，高い好奇心と意欲を持った学生，LSI の実設計やセキュリティに興味ある学生，自分の研究を国内外で発表したい学生を歓迎します．

・本資料で当研究室に興味を持った方は，是非 http://www.ritsumei.ac.jp/se/re/fujinolab/ （公開サーバー）や http://rh5pt200.bkc.ritsumei.ac.jp/wiki/ （研究室イントラネットサーバ）をアクセスしてみてください．メイルや訪問による質問も歓迎ですので fujino@se.ritsumei.ac.jp または kumaki@fc.ritsumei.ac.jp に連絡してください．