

【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&ハードウェア～

○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)

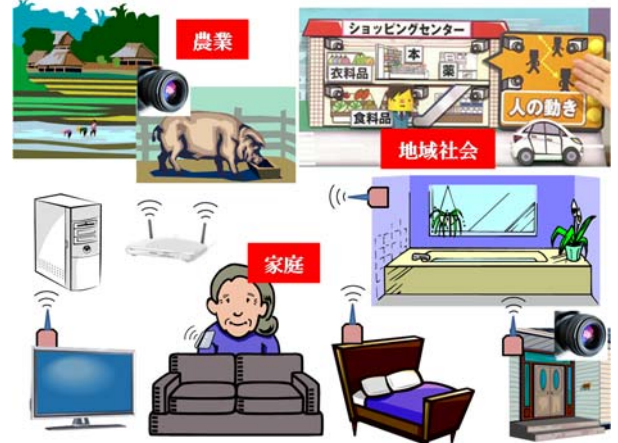


図2. 家庭・地域社会・農業で普及するセンサーネットワーク

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・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、2013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」のハードウェア&ソフトウェ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)、研究教員研究員(白畑、汐崎)、研究員(久保田)と大学院生9名、学部生10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

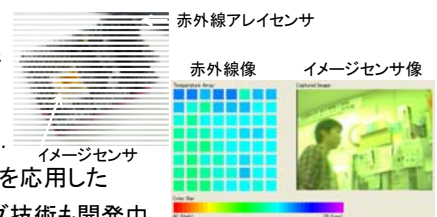
モバイル機器向け LSI の開発とその応用を行っている。

スマホ盗撮防止技術、電子透かし、画像マスク法、画像改竄防止、及びハードウェアトロイ等について研究。画像処理とFPGAや組込みプロセッサでデモシステムを作ります。学会や展示会、新聞やテレビで発表中。



<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。CMOS、及び赤外線カメラを搭載したGSSEというハードを中心に、人物検知技術やアナログ回路設計、評価システムを開発中。また、赤外線や超音波を応用しただまされないセンシング技術も開発中。



<PUF&SCA> 固有 ID 生成技術と耐タンパ暗号回路

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)技術が注目されている。また、暗号回路では、サイドチャネル攻撃による鍵情報の漏えいが問題となっており、攻撃手法や対策回路の研究を行っている。右図は PUF と AES 暗号回路を使用した、安全なキーレスエントリーデモシステムである。



<車載> 車載セキュリティ

スバルのアイサイトに代表される運転支援システムやグーグルの自動運転車に見られるように自動車のコンピュータ制御が非常に進歩している。一方でハッカーによる自動車の乗っ取りなどが話題になり、車載セキュリティが非常に話題となっている。右図は、車載ネットワークである CAN の通信に暗号化を用いて車の乗っ取りを防止するデモシステムである。



○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 に示すような盗撮防止システムを構築して、2015 年 6 月には組込みシステム展でデモンストレーションを行いました。新聞、ニュースでも注目され、各社新聞記事、yahoo ニュースやトレンドたまご、ニュース ten で紹介されました。現在は警察との連携を検討中です。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。

グランフロント大阪にて研究
を紹介。学生 5 人が参加

新聞記事（日経、読売、
朝日、産経、毎日等）

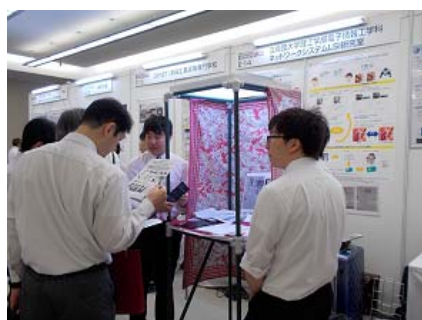


図 3. 盗撮防止及び、画像改ざん検知システム展示



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、英文書の輪講と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～2015 年の 3 年連続ハワイで行われた学会で当研究室の M2 および M1 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付けて、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。メー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。