【ネットワークLSIシステム（藤野・熊木）研究室】

～ 特徴あるLSIアーキテクチャとセキュリティー＆ネットワーク応用 ～

○研究紹介

大容量のメモリとマイクロプロセッサ等のロジック回路を，１チップの大規模集積回路(VLSI)上に実現した「システム LSI」は，さまざまな情報機器で使用される「小型低消費電力かつ高性能なシステムの実現」に必須の技術となっています．作りたいLSIの仕様が決定したら，あとは設計CADを使って簡単にシステムLSIは作成できると考えているかもしれないですが，実際に低消費電力・高性能・低コスト・高信頼性などの要求を満足しようとすると，新しい特徴あるLSIアーキテクチャが必要となってきます．

当研究室では，以下のようなLSIアーキテクチャの研究と応用を，教員（藤野，熊木），研究員（汐崎，Tuan），研究補助員（浅川）と大学院生20名が，他大学や，ルネサスエレ・三菱電機等の産業界と交流しながら行っています．

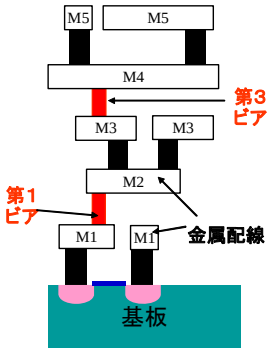
(1)ビアプログラマブルLSI設計<VP>　ブリティッシュコロンビア大学
(2)耐タンパLSI設計＆非接触電力転送<SCA>　CRESTプロジェクト（産総研，名城大学，三菱電機）
(3)マトリックス型超並列プロセッサ応用<MX>　ルネサスエレクトロニクス
(4)製造ばらつきを利用した固有ID生成技術<PUF>　CRESTプロジェクト（産総研，名城大学，三菱電機）

研究ターゲットとしているアプリケーションは，暗号・乱数等の符号処理および画像処理技術を使った認証・コンテンツ＆プライバシー保護を目標としており，今後ますます重要になるセキュリティー技術の知識を修得できます．

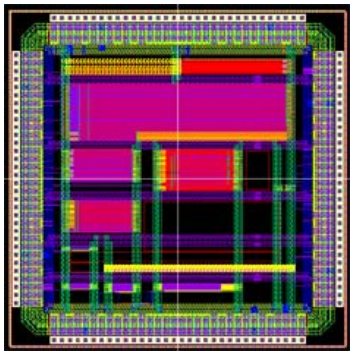
○研究テーマ説明図

(1) ビアプログラマブルLSI <VP>

現在，新しいLSIを試作する際には回路原版であるフォトマスク費用として，1億円以上のコストが必要である．本研究では，LSI製造工程のビア数層のレイアウトを変更し，様々なデジタル＆アナログ回路を実現するという，低コスト LSI 設計技術の実現を目標とする．電子ビーム描画を組み合わせると，マスクコスト0を実現でき「世界で1つしかないLSI」が製造可能となる．

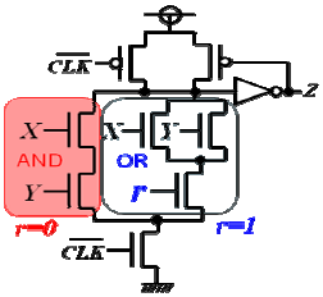


ウエハ断面構造

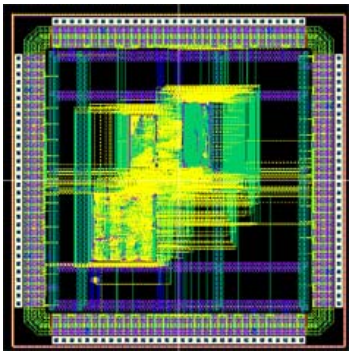


(2) 耐タンパLSI設計 <SCA>

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ドミノ型RSL回路や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．



ドミノ型RSLゲート

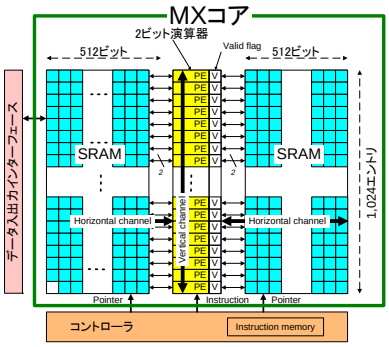


(3) マトリックス型超並列プロセッサの開発と応用 <MX>

最大1,024並列のデータ処理能力を誇るモバイル機器向け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，階層型画像マスク法，及びハードウェアトロイ等のアプリケーションについて研究中．また，超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．昨年度から発足した研究テーマであり，メンバーの様々なアイデアを積極的に採用する方針である．

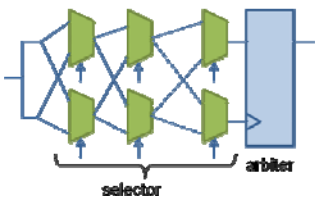
(4) 製造ばらつきを使用した固有ID生成技術 <PUF>

金銭情報を扱うLSIや，自動車などの生命を扱うLSIにおいてデバイスが不正に複製されると，社会的に大きな被害が生じる．これを防止するためにはデバイスごとに固有のIDを持たせることが必要である．当研究室ではLSIの製造ばらつきを利用した遅延時間差検出型アービターPUF(Physically Unclonable Function)を設計しID再現性・衝突耐性，学習攻撃耐性を評価している．

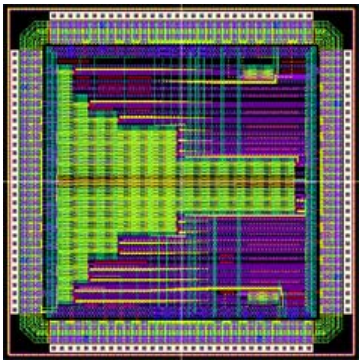


超並列MXコア

超小型マイコン実験ボード



アービターPUF回路



○使う研究設備

当研究室の大きな特徴は，**LSI を実際に作り評価する**というところです．LSI 設計用サーバー（8Core CPU, 64GB Memory）２台と設計ツール（業界標準のケイデンス，シノプシス，メンター社製）を駆使して，LSI を設計します．2010 年以降，0.18μm プロセスで 11 種類，今年は，三菱電機と共同で 65nm プロセスの LSI も設計しています．試作された LSI は，LSI 評価専用 FPGA ボードを用いて基本機能評価を行うほか，恒温槽を使って，温度を変化させた際の安定性なども評価しています．また，図１に示すように内部の暗号回路動作時の消費電力や電磁波を用いて秘密鍵を窃取するというサイドチャネル攻撃実験も行っています．LSI を作り，様々な評価を行うことを通して，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．

また図２に示すように FPGA や CPU が搭載されたボードを用いて，セキュリティー**システムのプロトタイプを構築し評価する研究**も行っています．ソフトウェア技術からハードウェア技術までを網羅して学ぶことができ，実際に動作させる楽しさを経験することができます．

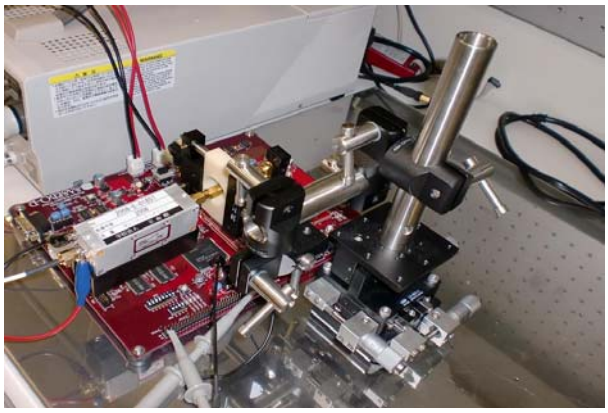


図１．電磁波を用いたサイドチャネル攻撃実験設備

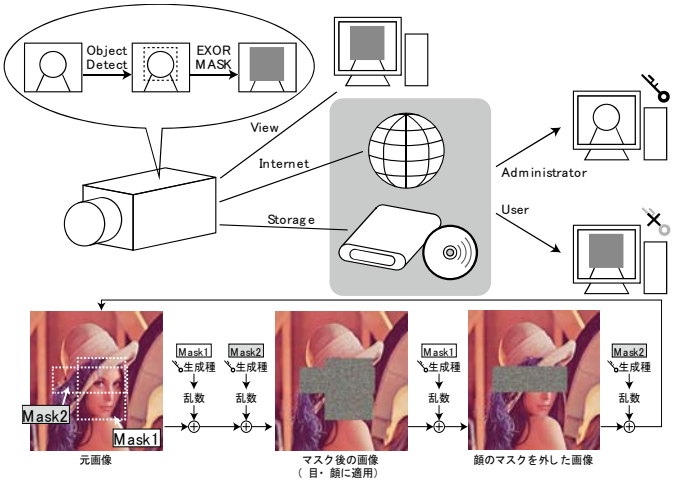


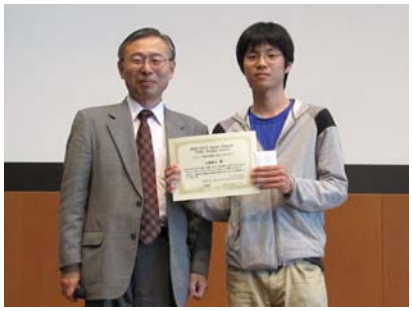
図２．監視カメラ向け階層型画像マスキングシステム

○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，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回路設計ツール実習を大学院生から週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，2010 年度に国内学会 23 件，国際学会 6 件を発表しました．また，今年５月には，VDEC（東京大学大規模集積システム設計教育研究センター）を通して全国で設計・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 が設計した「遅延時間差検出型アービター PUF」が競合大学とプレゼンで競った結果，最優秀賞を受賞しました．右写真はその時の光景です．（http://www.vdec.u-tokyo.ac.jp/designAward/welcome.html を見てください．）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あり，不思議かもしれないですが，学会発表で就活の時間が少なかった学生ほど，早く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ーに興味ある学生，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．