Rits 立命館大学

電子情報デザイン学科　藤野　毅
応用演習研究室紹介　2010.10.11

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
  - 助教：熊木　武志（小倉研と兼任）
  - 研究員：汐崎　充，Hoang Anh Tuan
  - 研究補助員：浅川　俊介，松田　詩織（秘書）
  - (M2)：2名，(M1)：10名
  - 学部学生(B4)：14名（11名がM1に進学予定）

2

4つの研究テーマ領域

（1）ビアプログラマブルLSI設計<VP>
- ビア数層をEB直描でプログラムして任意のロジック回路を作製
- 「世界で一つしかないLSI」を安価に製造可能

（2）耐タンパLSI設計＆非接触電力転送<SCA>
- ICカード内の暗号回路の消費電力・放射電磁波を解析して機密情報を窃取する「サイドチャネル攻撃」を阻止する設計技術
- ICOCA，PiTaPaなどで使われている非接触給電も開発中

（3）マトリックス型超並列プロセッサ<MX>
- ルネサスが開発した1024個の演算器を持つ超並列SIMD
- ARM系SIMD，GPU，FPGA などと演算能力・消費電力を比較

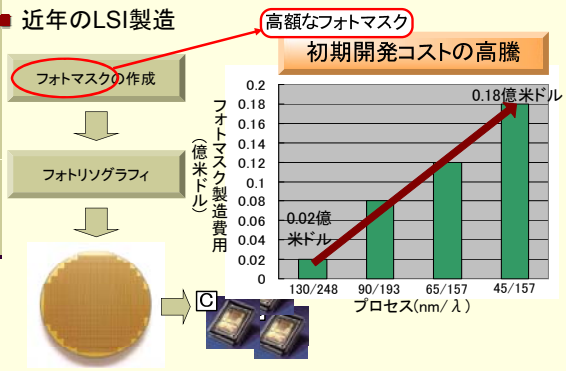
（4）製造ばらつきを利用した固有ID生成技術<PUF>
- ICカード，高性能LSIなどの偽造防止用IDを発生する技術
- LSI製造時のトランジスタ性能などのばらつきを利用

3

VP

VPEXの研究背景(1)

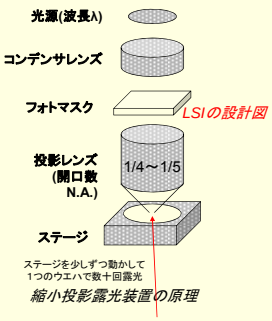
- 近年のLSI製造



4

VP

パターン転写装置（光転写）



縮小投影露光装置の原理

光転写装置(ステッパー)外観

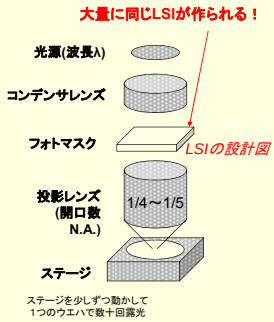
大量に同じLSIが作られる！

＊栃木ニコンホームページより引用

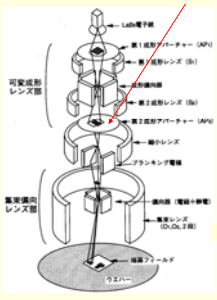
5

VP

マスクレス描画（EB直描）



フォトマスクを使った光露光



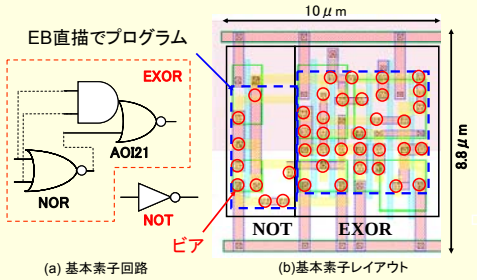
マスクレスEB描画

6

VP

VPEX（Via Programmable logic device using EXclusive-or array）

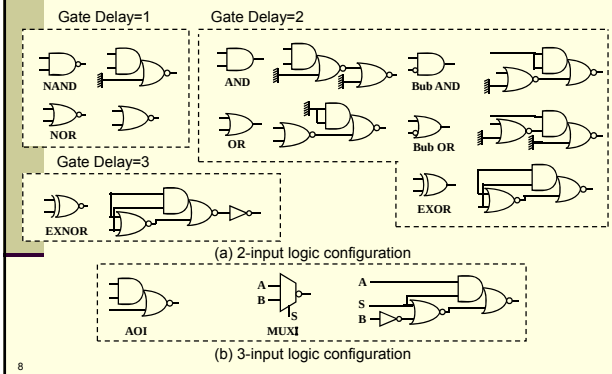
- 複合ゲート型XORゲートをベースに素子を構成
  - 論理を出力するために、入力、出力端子を分割
  - Via1の変更だけで、12種の論理が出力可能



7

VP VPEX

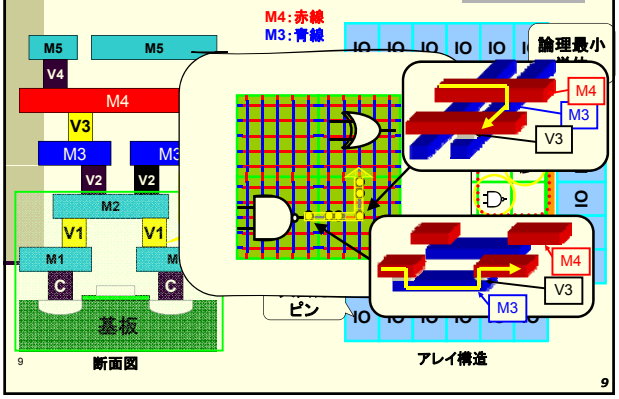
基本素子から出力できる論理（全12種類）



8

VP

VPEXのアーキテクチャ

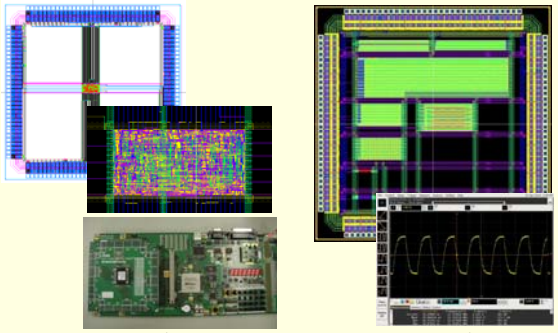


9

VP

VPEX テストチップ

- Rohm 0.18μmCMOS



初代機能評価チップ(VPEX1)　2代配線遅延評価チップ(VPEX2)

10

4つの研究テーマ領域

（1）ビアプログラマブルLSI設計<VP>
- ビア数層をEB直描でプログラムして任意のロジック回路を作製
- 「世界で一つしかないLSI」を安価に製造可能

（2）耐タンパLSI設計＆非接触電力転送<SCA>
- ICカード内の暗号回路の消費電力・放射電磁波を解析して機密情報を窃取する「サイドチャネル攻撃」を阻止する設計技術
- ICOCA，PiTaPaなどで使われている非接触給電も開発中

（3）マトリックス型超並列プロセッサ<MX>
- ルネサスが開発した1024個の演算器を持つ超並列SIMD
- ARM系SIMD，GPU，FPGA などと演算能力・消費電力を比較

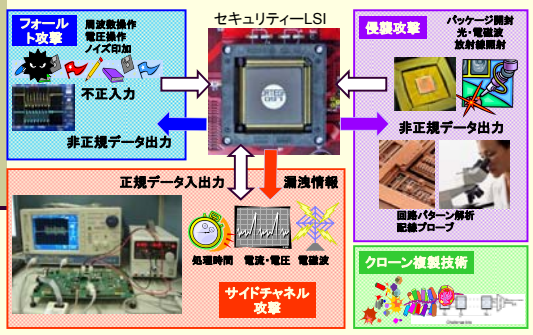
（4）製造ばらつきを利用した固有ID生成技術<PUF>
- ICカード，高性能LSIなどの偽造防止用IDを発生する技術
- LSI製造時のトランジスタ性能などのばらつきを利用

11

SCA

耐タンパディペンダブルLSIの要件

- 下記のような物理攻撃・複製技術に対して耐性のあるセキュリティーLSI

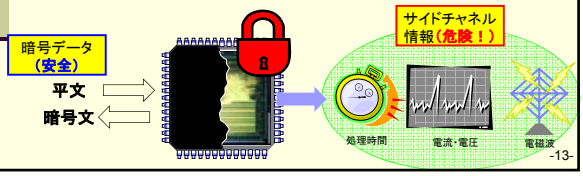


12

SCA

暗号処理回路とサイドチャネル情報

- 暗号鍵が機密情報を守る
- 標準暗号　3DES，AES
  ⇒　暗号アルゴリズムは公開
  ⇒　多くの研究者によって数学的な安全性は保証
- 暗号回路動作時のサイドチャネル情報
  - サイドチャネル情報＝処理時間．消費電力，電磁波
  - サイドチャネル情報から暗号鍵を推定



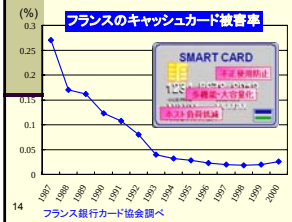
13

-13-

SCA

暗号モジュールの用途

- ICカード・RFID・電子パスポート
- 暗号ネットワーク通信
- 音楽・映像メディアのコンテンツ保護
- ビジネス文書・FPGAの設計情報の保護



14

SCA

LSIの新しい使われ方～電子マネー～

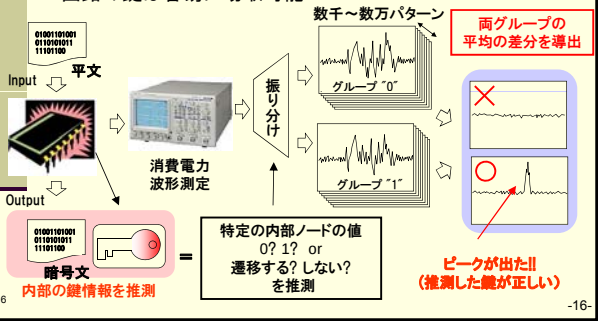
- 非接触型ICカード：Felica（ソニー）
  - 記憶できる情報量が多く、また演算機能もあるため、コンピューター並みの高機能を実現
  - 偽造・変造防止といった高度なセキュリティー機能を持つ
  - バッテリーレス・非接触で動作させることができる
- IC乗車カードSuica（JR東日本）ICOCA（JR西日本）として、「かざすだけ」で改札を通過できるため爆発的に普及．
- 2005年硬貨流通量の減少が起こった

15

SCA

電力利用サイドチャネル攻撃（DPA）

- 1999年にKocherらによって提案された電力差分解析(DPA)攻撃により，未対策回路では，実際に共通鍵暗号回路の鍵は容易に窃取可能



16

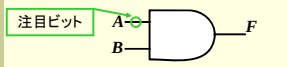
-16-

SCA

電力利用サイドチャネル攻撃の原理

耐タンパ

- 単純な2入力ANDゲートの場合
  A1⇒A2，B1⇒B2，の遷移は2^4＝16通り



A_1=0のときの遷移確率　2/8

1/4回電力増加

消費電力に差が出る

A_1=1のときの遷移確率　4/8

1/2回電力増加

注目ビットの値を推定し，注目ビットが1の場合と0の場合の消費電力に差が生じれば推定値は正しい

A_1	B_1	A_2	B_2	F_1	F_2	
0	0	0	0	0	0	
0	0	0	1	0	0	
0	0	1	0	0	0	
0	0	1	1	0	1	遷
0	1	0	0	0	0	
0	1	0	1	0	0	
0	1	1	0	0	0	
0	1	1	1	0	1	遷
1	0	0	0	0	0	
1	0	0	1	0	0	
1	0	1	0	0	0	
1	0	1	1	0	1	遷
1	1	0	0	0	0	
1	1	0	1	1	0	遷
1	1	1	0	1	0	遷
1	1	1	1	1	1	

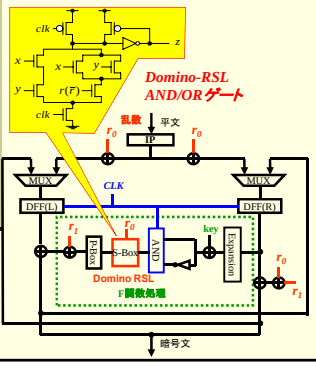
17

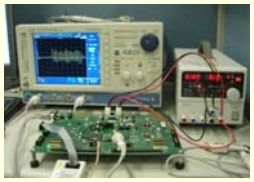
-17-

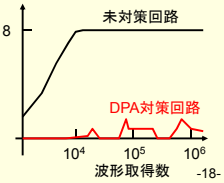
SCA

消費電力サイドチャネル攻撃耐性目標

- 擬似Domino-RSLゲートを用いた暗号回路をFPGA実装して評価







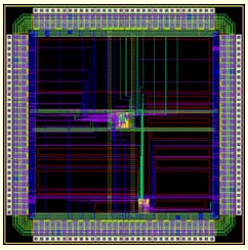
18

-18-

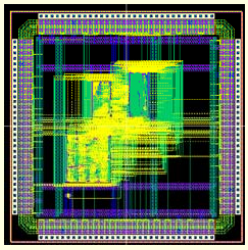
SCA

ドミノRSL回路を用いた暗号チップ

- ローム0.18μmCMOS



簡易DES暗号回路
（すべてマニュアル設計）



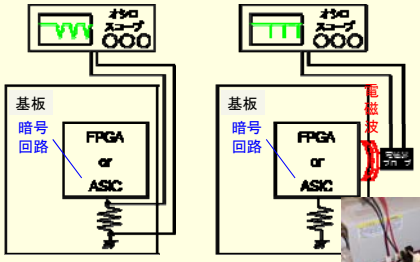
DES暗号回路
（自動配置配線ツール適用）

19

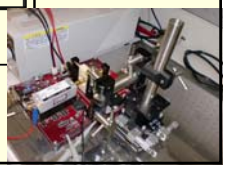
SCA

漏洩電磁波での攻撃DEMA

消費電力を直接測定　電磁波で間接的に測定



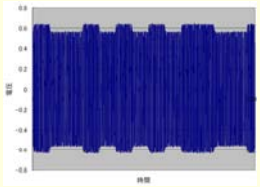
電源端子のない非接触ICカードで有効な攻撃

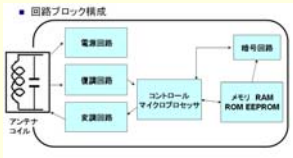


20

ワイアレス給電システム

- ICカードの給電





21

4つの研究テーマ領域

（1）ビアプログラマブルLSI設計<VP>
- ビア数層をEB直描でプログラムして任意のロジック回路を作製
- 「世界で一つしかないLSI」を安価に製造可能

（2）耐タンパLSI設計＆非接触電力転送<SCA>
- ICカード内の暗号回路の消費電力・放射電磁波を解析して機密情報を窃取する「サイドチャネル攻撃」を阻止する設計技術
- ICOCA，PiTaPaなどで使われている非接触給電も開発中

（3）マトリックス型超並列プロセッサ<MX>
- ルネサスが開発した1024個の演算器を持つ超並列SIMD
- ARM系SIMD，GPU，FPGAなどと演算能力・消費電力を比較

（4）製造ばらつきを利用した固有ID生成技術<PUF>
- ICカード，高性能LSIなどの偽造防止用IDを発生する技術
- LSI製造時のトランジスタ性能などのばらつきを利用

22

MX

MX (Massive-Parallel SIMD Matrix)

23

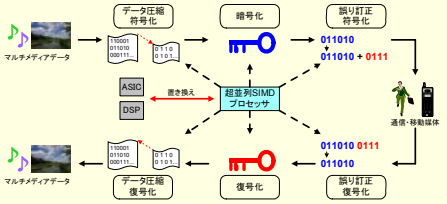
MX

研究背景

マルチメディアデータ処理LSIに求められる技術
- リアルタイムデータ処理：デジタルテレビは100 Mbyte/sのコーディングが必要
- プログラマブル処理：携帯電話にゲーム，音楽，TV及び電子マネー，etc.
  通信方式等仕様の変更が多い．
- 低消費電力：長時間駆動

従来のハードワイヤードIPでは対応が困難，組み込みマイコンでは処理性能が不足

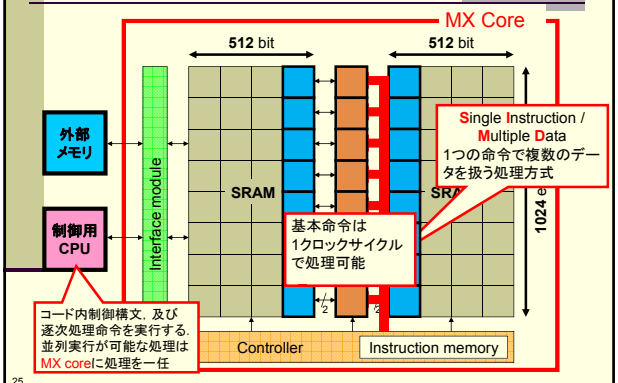
マルチメディアに特化し，高性能かつ低消費電力なプログラマブルデバイスが必要



24

MX

マトリックス型超並列プロセッサ (MX-1)



25

25

MX

研究状況 1/2

現在4つのテーマをメインに研究中

- MXを用いた暗号処理
  - ガロア体を利用したSubBytes変換による，高速AES処理
  - 参加人員: 吉川弘起，黒川悠一郎，本田　弘
- MXを用いた並列乱数処理
  - Mersenne Twisterの並列化による高速化処理
  - 参加人員:松本直樹，吉田直之，望月陽平
- MXを用いた情報ハインディング処理
  - 電子透かし，及びステガノグラフィの高速処理
  - 参加人員:大澤昌弘，海山智並
- Beagle Boardを用いたアプリケーション処理
  - 環境立ち上げ，及び並列AES実装
  - 参加人員: 黒川悠一郎，梶本寿明

上記の他，積極的に有効な実装アプリケーションをサーベイ中

MX

研究状況 2/2

- これまで実装研究を行ったアプリケーション
  - 離散コサイン変換 (DCT)
  - 高速乗算処理
  - 顔検出処理
  - ハフマン符号化
  - AES (S-Box使用)
- ルネサスエレクトロニクスと共同研究中！
  積極的に推進力になってくれる人を求めています．
  社会人との交流の機会あり．
  あなたのアイデアを民生品に反映させよう！

27

MX

研究成果発表状況 (4月から)

論文1件，国際学会2件，及び国内学会3件

- 論文誌 (査読中)
  - “Software-based parallel Cryptographic Solution with Massive-Parallel Memory-Embedded SIMD Matrix Architecture for Data-Storage Systems”, IEICE Trans (D), Takeshi Kumaki, et al.
- 国際学会発表，及び査読中
  - “Realization of Efficient and Low-Power Parallel Face-Detection with Massive-Parallel Memory-Embedded SIMD Matrix”, MWSCAS2010, Takeshi Kumaki, et al.
  - “Galois-Field Operation-Based Parallel SubBytes Transformation with Massive-Parallel SIMD Matrix”, ISCAS2011, Takeshi Kumaki, et al.
- 国内学会発表
  - “超並列SIMD型演算プロセッサMX-1へのMersenne Twisterの実装 (1)”, 2010年ソサイエティ大会，吉田直之他
  - “超並列SIMD型演算プロセッサMX-1へのMersenne Twisterの実装 (2)”, 2010年ソサイエティ大会，松本直樹他
  - “超並列SIMD型演算プロセッサMX-1のためのガロア体演算によるAES用SubBytes変換の高速化”, 2010年ソサイエティ大会，吉川弘起他

28

MX

研究成果発表状況 (4月から)

29 ソサイエティ大会@大阪府立大

MWSCAS2010@シアトル

MX

質問，見学は気軽にどうぞ

©蛙男商会

4つの研究テーマ領域

(1)ビアプログラマブルLSI設計<VP>
- ビア数層をEB直描でプログラムして任意のロジック回路を作製
- 「世界で一つしかないLSI」を安価に製造可能

(2)耐タンパLSI設計＆非接触電力転送<SCA>
- ICカード内の暗号回路の消費電力・放射電磁波を解析して機密情報を窃取する「サイドチャネル攻撃」を阻止する設計技術
- ICOCA，PiTaPaなどで使われている非接触給電も開発中

(3)マトリックス型超並列プロセッサ<MX>
- ルネサスが開発した1024個の演算器を持つ超並列SIMD
- ARM系SIMD，GPU，FPGA などと演算能力・消費電力を比較

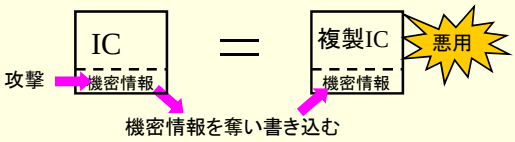
(4)製造ばらつきを利用した固有ID生成技術<PUF>
- ICカード，高性能LSIなどの偽造防止用IDを発生する技術
- LSI製造時のトランジスタ性能などのばらつきを利用

31

PUF

研究背景

- 近年ICカードは様々な所で使われており、IC内のメモリなどに秘密情報を格納することで安全性を保障
- 秘密情報はサイドチャネルアタックなどの攻撃により窃取される危険がある
- その情報をもとに、複製・偽造することが可能であり、悪用される危険性が指摘されている→対策が必要



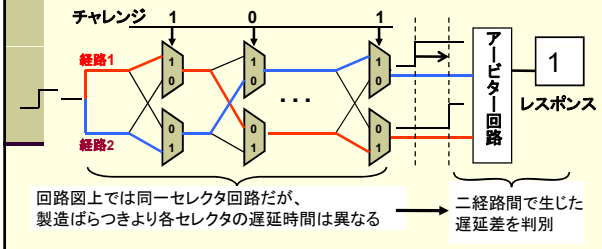
- 偽造防止デバイスとして、**Physical Unclonable Functions (PUF)**と呼ばれる技術が注目されている

2

PUF

アービターPUF

- アービターPUFは製造ばらつきによる遅延特性の差異を用いたPUFの一種

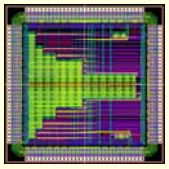


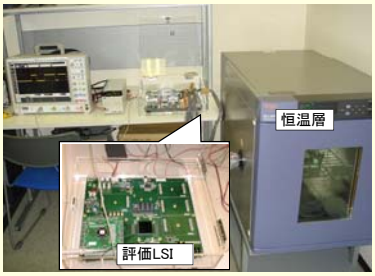
4

PUF

チップと評価システム

- ID再現性，ID衝突耐性を評価中





34

PUF

LSIの新しい使われ方～電子タグ～

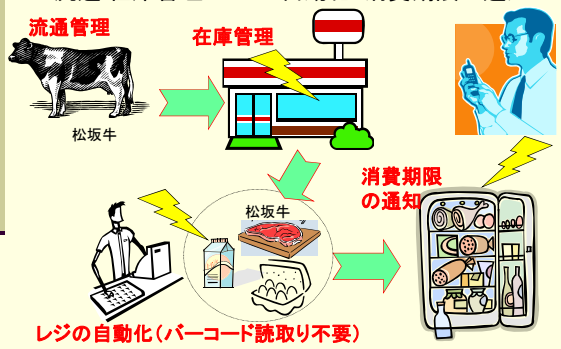
- 非接触型電子タグ：μチップ（日立）
  - シンプルな機能：読み取り専用
  - 個品管理対応可能（低コスト）
  - データ格納：128ビットユニークID（製造時に設定）
  - 通信特性：周波数2.45GHz、最大距離約30cm
  - 受動型：電池無しで動作
- 愛知万博の入場券で使用．今後物流管理，在庫管理，セキュリティーなどさまざまな用途．

35

PUF

電子タグの応用

- 流通/在庫管理・レジの自動化・消費期限の通知



36

卒論までのながれ

応用演習	2010/12-2011/1	・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12/20予定）
輪講ゼミ	2011/2-2012/1	週1回「Introduction to VLSI Circuits and Systems」を読み進めます
春季演習 （週1回）	2011/2-3	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）	2011/4-6	・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	2011/6-7	院生ゼミの結果から希望調査 夏休みから本格研究開始 6～7月に最終決定（B4学生発表）
卒論目次作成	2011/12	卒論作成前に内容を整理，中間発表
卒論提出	2012/2	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
  - 今年度のB4は11/14名が大学院進学予定
- 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ーシンポジウム」
  - M2は海外発表・論文誌投稿が目標
- 対外研究交流
  - ビアプログラマブルロジックVPEX:UBC
  - 耐タンパLSI設計技術,PUF：産総研，名城大
  - 超並列SIMD MX：ルネサスエレクトロニクス
- 過年度（2006-2009）の修士の就職先
  - 東芝6，日立3，ローム3，ネットワンシステムズ2　他

38

研究室訪問・見学

- 今週（アポイントメントなし，個人研究室,藤野1・3研）
  - 10/11（月）　18:00～19:00（このあとすぐ）
  - 10/14（木）　13:30～14:30, 18:00～19:00

  ＊上記以外の個別相談はメイルで予約してください
- 配属希望調査前（詳細はHPで確認してください）
  - **11/1(月) 16:20～17:50（応用演習時間帯）
研究室見学＆教員面談@藤野2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．
  - **11/8(月) 16:30～18:00（応用演習時間帯）
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を行う予定です．
（1）ビアプログラマブルLSI設計<VP>
（2）耐タンパLSI設計＆非接触電力転送<SCA>
（3）マトリックス型超並列プロセッサ<MX>
（4）製造ばらつきを利用した固有ID生成技術<PUF>

39

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・ハードの総合的な理解ができる
- 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/

40