

---

電気・電子情報工学系 情報通信システム分野

# 専用計算システム研究室

研究室紹介・2025年度版

教授・市川 周一 [ichikawa@tut.jp](mailto:ichikawa@tut.jp)

# 担当教員： 市川 周一（教授）

手段

- ・ 計算機アーキテクチャ
  - マイクロプロセッサ, 並列計算機
- ・ **専用計算回路**, 応用指向計算
  - 組込みシステム, 計算困難問題
- ・ 再構成可能論理
  - **FPGA**, データ依存回路技術
- ・ 高性能計算
  - 並列処理, クラスタ, 負荷分散
- ・ セキュリティ
  - 暗号回路, 乱数回路, セキュアシステム
  - 情報隠蔽, 電子署名

共通の目標は...

**高速処理**

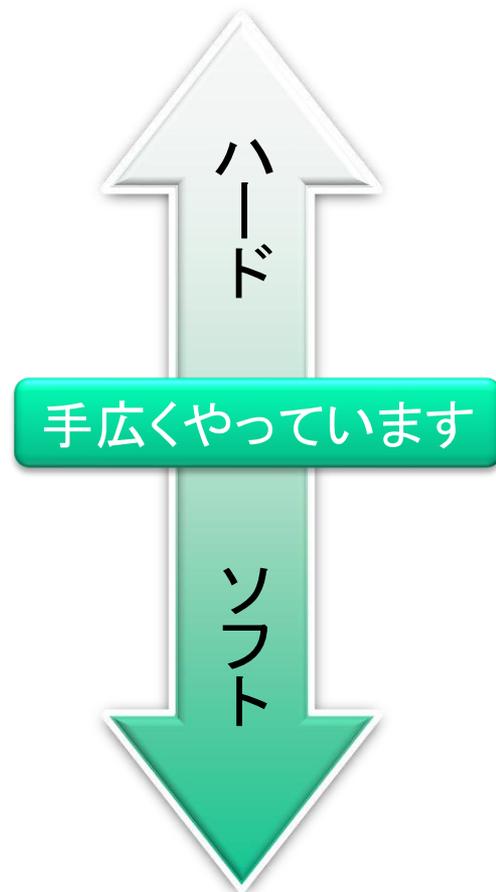


応用

# 研究分野

---

- ハードウェア方面
  - 再構成可能計算機システム
  - 専用回路による応用の高速化
  - 組込みシステム
  - セキュアシステム
- 応用ソフトウェア方面
  - 並列処理, 広域分散処理
  - 高性能計算手法, 最適化手法
  - 情報とシステムのセキュリティ



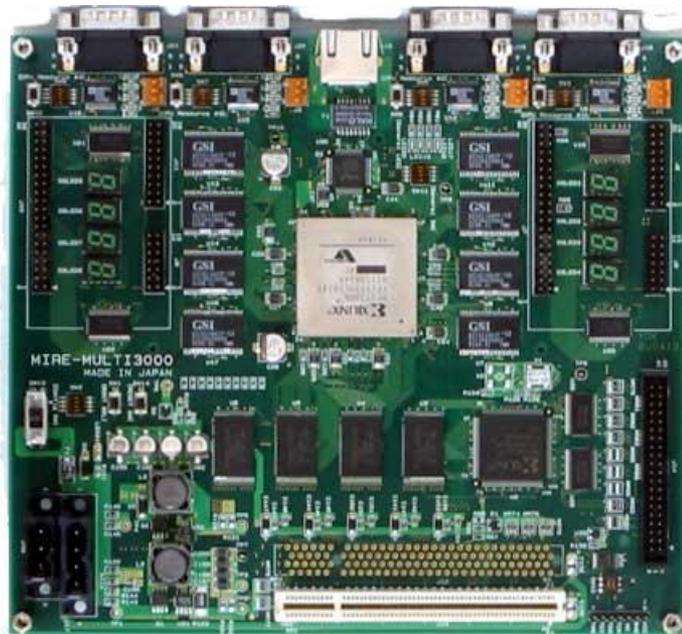
# 重点的に進めている研究テーマ

---

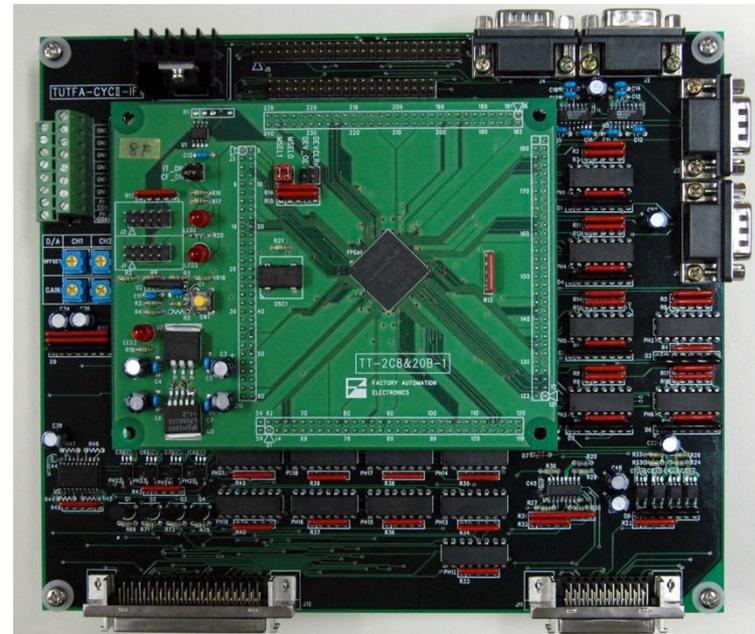
- 再構成可能論理を用いた専用回路
  - FPGAを用いて応用プログラムを高速化
  - 計算困難問題, 産業機械への応用
- セキュアシステムの研究
  - ソフトウェアのハードウェア化による秘匿性向上
  - セキュアプロセッサ
  - 乱数生成回路
  - 電子透かし, 情報隠蔽
- 並列処理技術
  - 近年のマルチコア／メニーコアシステムの利用技術
  - 組込み応用, 組込みシステムの高性能化

# 再構成可能論理システム

- FPGAというLSIは何度でも書き換え可能  
– ソフトウェア開発のようにハードウェア開発



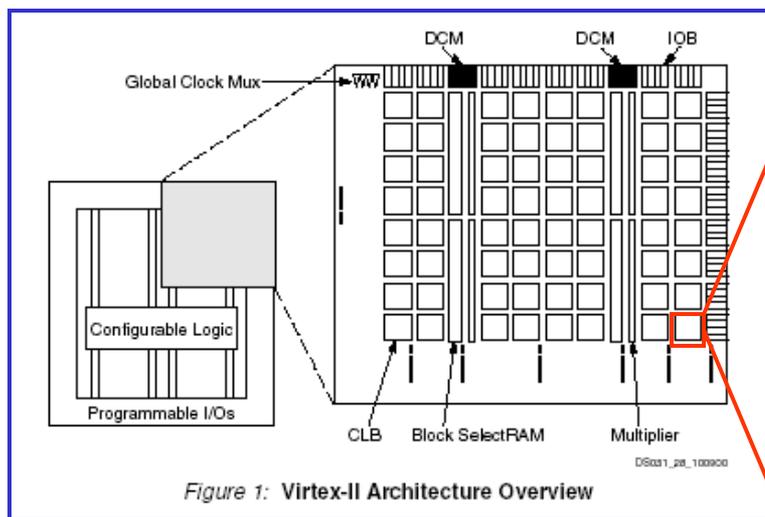
マルチプロセッサ評価ボード (2002年度製作)



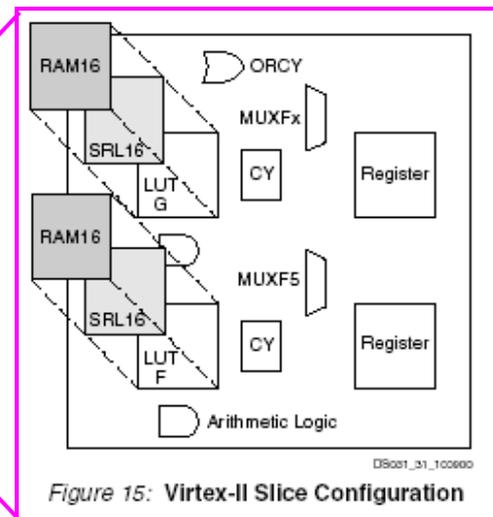
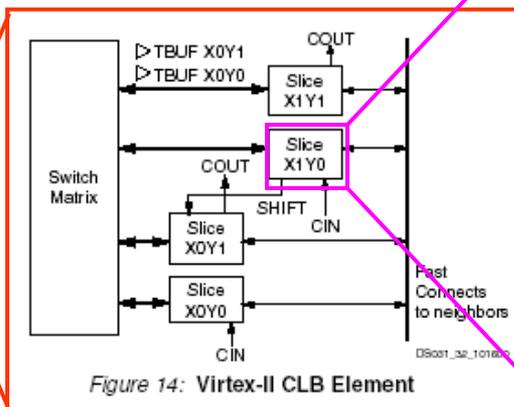
FPGA制御ボード (2006年度製作)

# 参考： Field Programmable Gate Array (FPGA)

- プログラム可能なLSI
  - 動作中でも，機能を何度でも変更できる
  - 極端に言うと，RAMとスイッチの塊

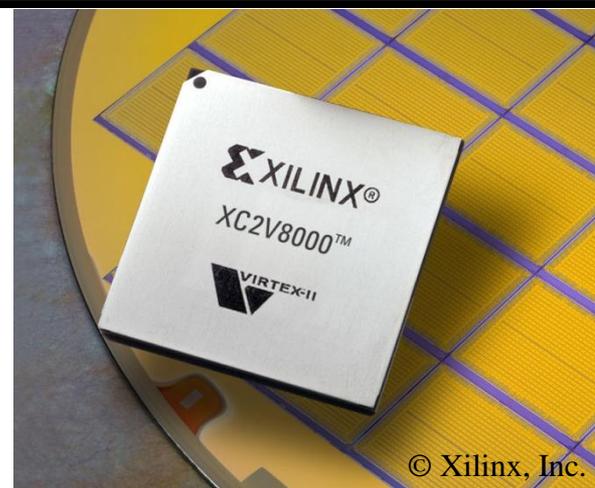


図： © Xilinx, Inc.



# 参考：FPGAとASIC

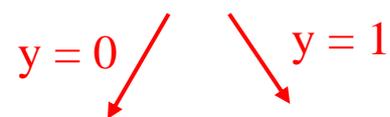
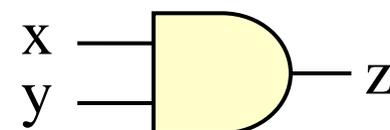
- ASIC, カスタムLSI
  - ロット単位の生産
  - 単価は下がる
  - 設計変更のコストが高い
  - 集積度は高い, 比較的高速
- FPGA
  - 一品生産, フィールド・アップグレード可能.
    - 動作中に再構成することも可能(動的再構成)
  - 集積度が向上した. 数十～数百万ゲート.
  - 速度も向上した. 数百MHzでのシステム動作も可能.
  - 最先端のプロセスが使用されている



# 専用回路への応用

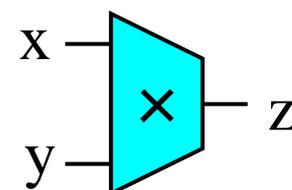
- 専用回路
  - 計算困難問題の高速化
  - 未解決問題の検証
- データ依存回路・特殊化
  - 回路の小型化と高速化
    - 部分グラフ同型問題
    - 暗号回路
  - ソフトウェアをハードウェアに自動で変換する研究

## 定数伝播

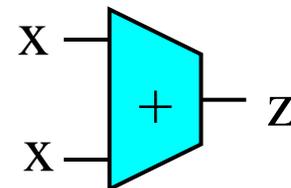
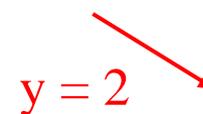


$0$  —  $z$

$x$  —  $z$

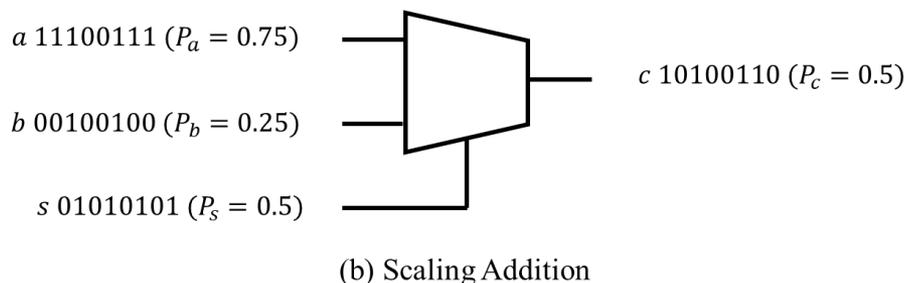
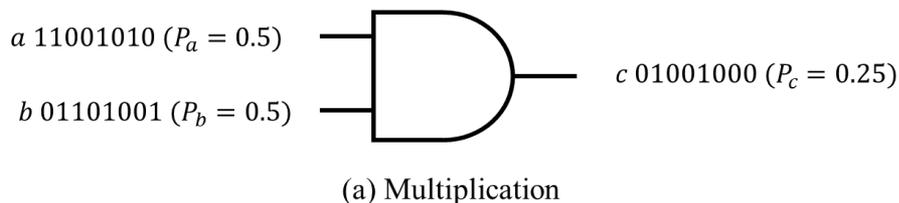


Strength  
reduction



# Stochastic Computing

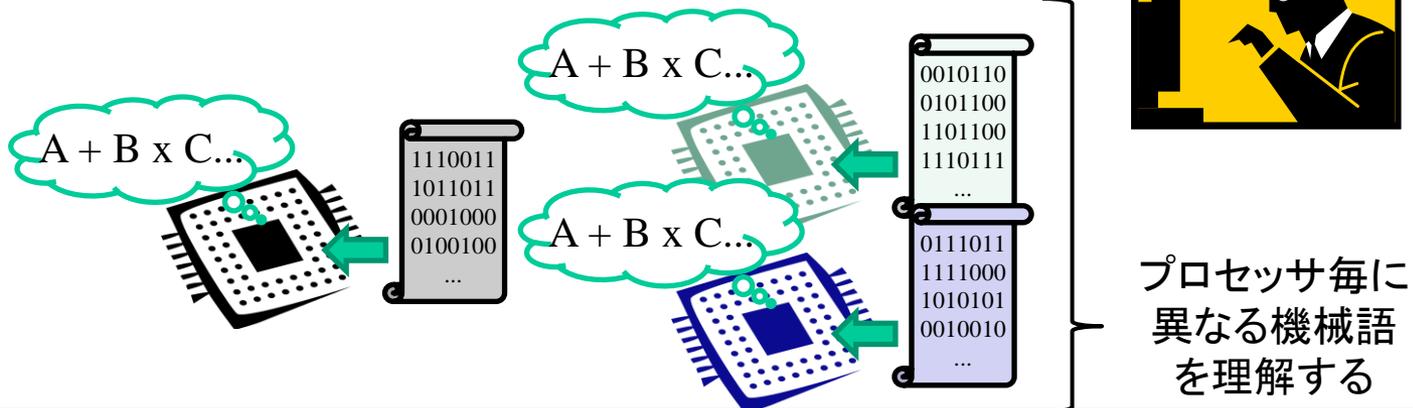
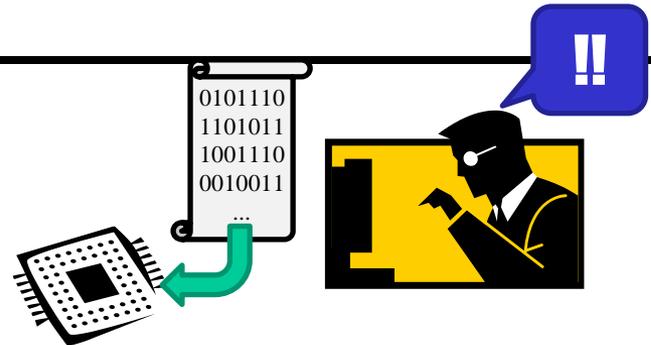
- 確率に基づく計算スキーム. 近似計算の一種.
- 画像処理, 通信, NNなどに適すると言われる
- 演算回路や消費電力が小さい



別役拓哉, 市川周一: "確率的計算を用いたGated Recurrent Unit の検討," 電気学会次世代産業システム研究会, IIS-25-005 (2025).  
鹿野貴義, 市川周一: "ストカスティック計算による画像フィルタ専用命令の実装," 電気学会次世代産業システム研究会, IIS-25-004 (2025).

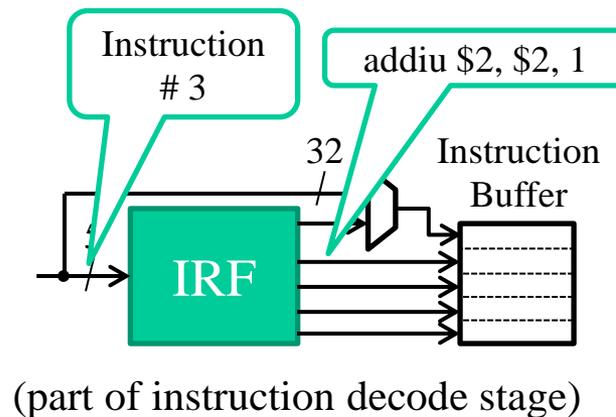
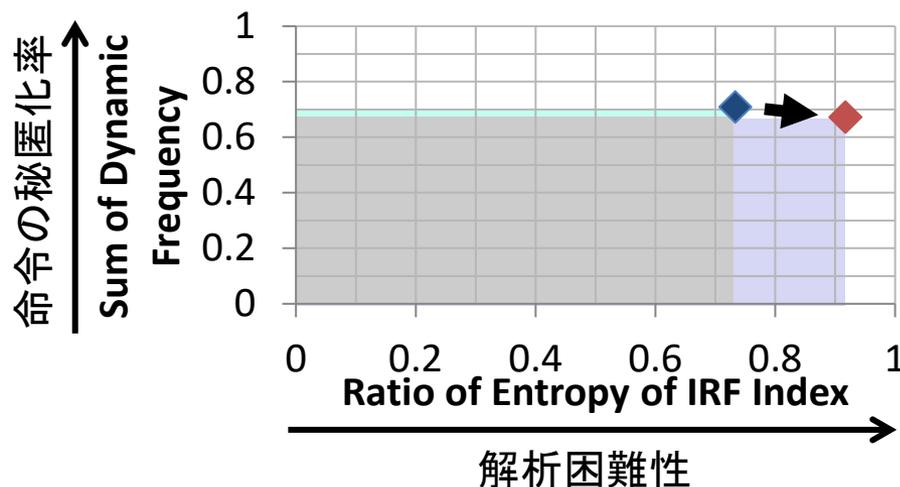
# セキュアプロセッサ

- ソフトウェアの解析・盗用・改ざん
  - 機密情報流出・海賊版流布のリスク
  - ソフトウェア保護を提供するプロセッサ (セキュアプロセッサ) の需要
- 多様化 に基づいたセキュアプロセッサ
  - 1つ1つが少しずつ異なる別々のプロセッサ
  - FPGAとの親和性が高い！



# IRFを用いた命令列の多様化

- 命令レジスタファイル (IRF)
  - よく使われる機械語を記録, 呼び出し
  - 電話で言うところの「短縮ダイヤル」
- IRFの命令リストを多様化する
  - リストに載せる命令を適切に選ぶと, 解析困難性が向上

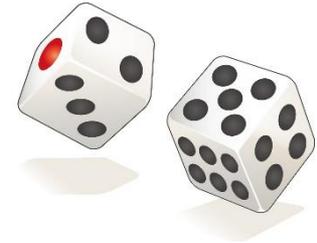


# 乱数生成器

## Random Number Generator

---

- 多くの応用で乱数生成は必須
  - シミュレーション, ゲーム, 等
- 真性乱数生成器 (TRNG; True RNG)
  - 物理現象から生成される. 予測不能.
    - 熱雑音, メタスタビリティ, ジッタ, ...
  - 専用ハードウェアが必要
- 疑似乱数生成器 (PRNG; Pseudo-RNG)
  - アルゴリズムと初期値で生成される. 予測可能.
- Unpredictable RNG (URNG)
  - TRNGとPRNGの中間, 実質的に予測不能.
  - プロセッサに専用レジスタを追加する, など



Naoki Fujieda, Shuichi Ichikawa, Ryusei Oya, Hitomi Kishibe: "Design and implementation of an on-line quality control system for latch-based true random number generator," IEICE Transactions on Information and Systems, vol. E106-D, no. 12, pp.1940-1950 (2023).

Shunsuke Matsuoka, Shuichi Ichikawa, Naoki Fujieda: "A true random number generator that utilizes thermal noise in a programmable system-on-chip (PSoC)," International Journal of Circuit Theory and Applications, vol. 49, no. 10, pp. 3354-3367 (2021).

# 乱数生成器

## Random Number Generator

- 多くの応用で乱数生成は必須
  - シミュレーション, ゲーム, 等
- 真性乱数生成器 (TRNG; True RNG)
  - 物理現象から生成される. 予測不能.
    - 熱雑音, メタスタビリティ, ジッタ, ...
  - 専用ハードウェアが必要
- 疑似乱数生成器 (PRNG; Pseudo-RNG)
  - アルゴリズムと初期値で生成される. 予測可能.
- Unpredictable RNG (URNG)
  - TRNGとPRNGの中間, 実質的に予測不能.
  - プロセッサに専用レジスタを追加する, など



別役拓哉, 市川周一: "LFSRを用いたURNGにおける風向データの削減," 電気学会論文誌D, vol. 145, no. 4, (to appear) (2025).

市川周一: "画像データとLFSRによる乱数生成手法," 電気学会論文誌D, vol. 145, no. 4, (to appear) (2025).

Ayumu Chiba, Shuichi Ichikawa: "Random number generation based on cryptocurrency prices and linear feedback shift register," Proc. Twelfth International Symposium on Computing and Networking (CANDAR 2024), pp. 142--148 (2024).

鴨狩混斗, 市川周一: "内蔵LFSRを用いた乱数生成方法の評価," 電気学会論文誌D, vol. 143, no. 2, pp. 87--93 (2023).

千葉歩武, 市川周一: "気象データとLFSRによる乱数生成手法の評価," 電気学会論文誌D, vol. 143, no. 2, pp. 80--86 (2023).

Shuichi Ichikawa: "Pseudo-Random Number Generation by Staggered Sampling of LFSR," Proc. Eleventh International Symposium on Computing and Networking (CANDAR 2023), pp. 134--140 (2023).

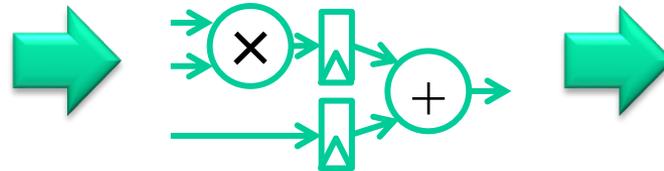
# 背景： 高位合成

---

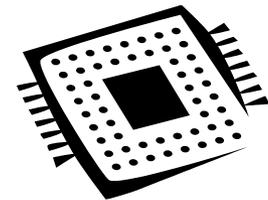
- ソフトウェアからハードウェアを生成する技術
  - 例: C言語 → ハードウェア記述言語
  - 歴史は古い(90年代～)が近年成熟しつつある

$D = A * B + C;$

プログラム



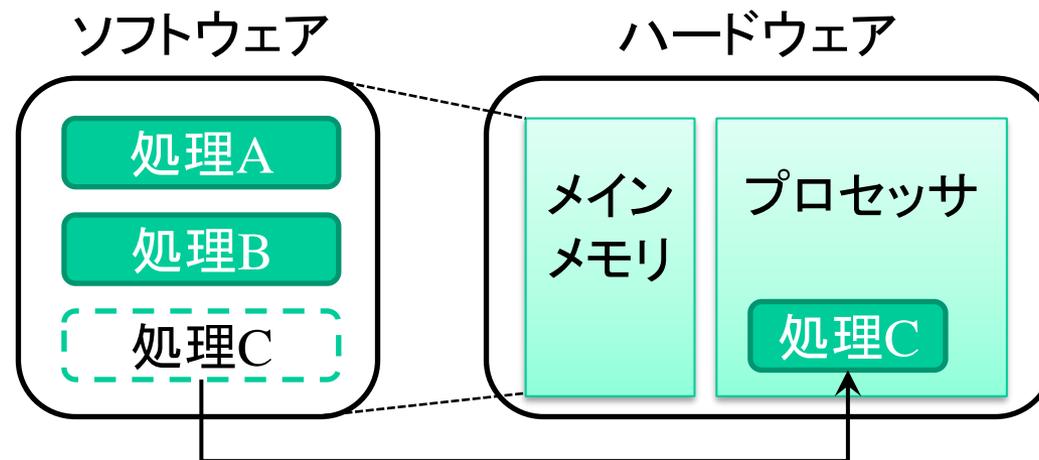
論理回路  
(ハードウェア記述)



ハードウェア

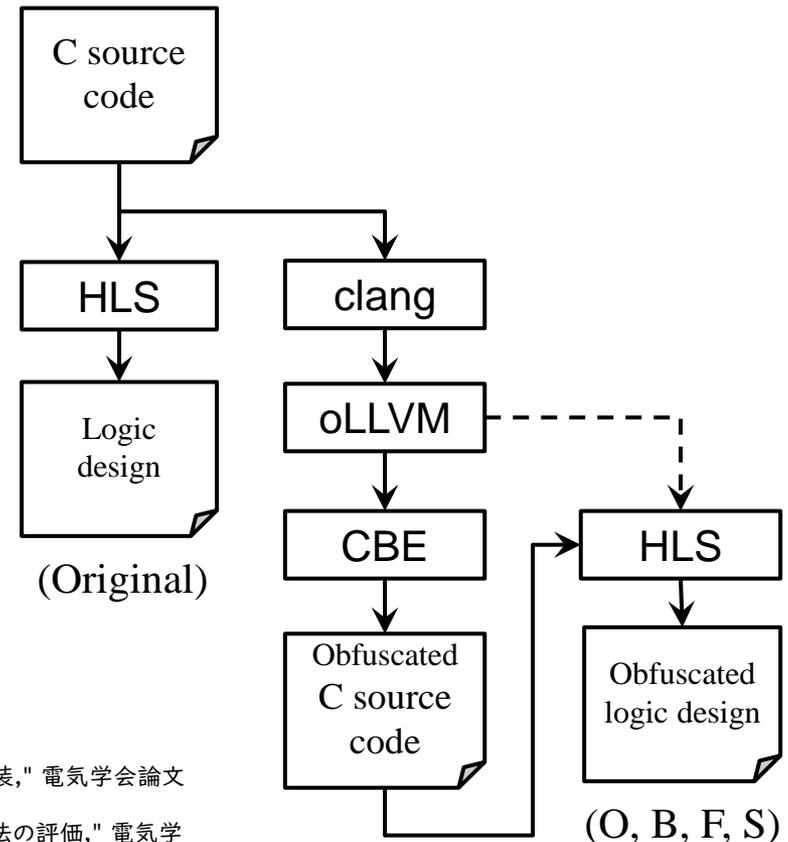
# 高位合成によるプロセッサ特殊化

- ソフトウェア処理の一部をプロセッサに組入れ
  - プロセッサもソフトウェアで記述 → 組入れ容易
  - 処理をプロセッサごとハードウェア化 → 解析困難
  - コンセプトを実証(2017~2021年度)



# oLLVMを用いたハードウェア難読化手法の評価

- 難読化(obfuscation)とは
  - プログラムを等価に変形することにより、攻撃者による理解や解析を妨げること
- LLVMはコンパイラ基盤
  - 言語やプラットフォームに依存しない
- oLLVM
  - LLVM上でソフトウェアの難読化を施すツール
- C言語ベースの論理設計記述をoLLVMで難読化し、高位合成(HLS)ツールで論理合成
  - 難読化されたハードウェアが生成可能
- 生成された難読化H/Wのオーバヘッドを評価した
  - 速度の低下, 論理規模の増大



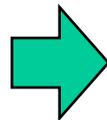
山田翔太郎, 市川周一, 藤枝直輝: "LegUpとoLLVMによる難読化制御論理回路の実装," 電気学会論文誌C, vol. 139, no. 9, pp. 952--957 (2019).

松岡佑海, 藤枝直輝, 市川周一: "難読化ツールoLLVMを用いたハードウェア難読化手法の評価," 電気学会論文誌D, vol. 139, no. 2, pp. 111--118 (2019)

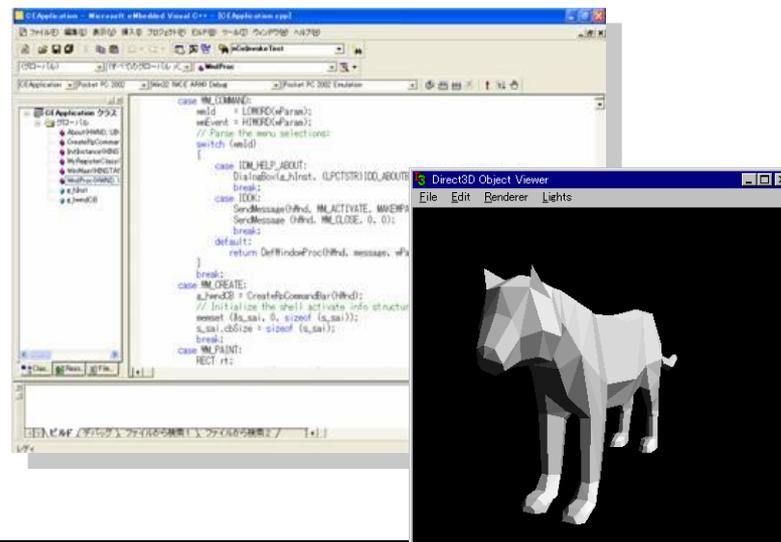
# 電子透かし・情報隠蔽

- 電子的著作物（例：プログラム・立体モデル等）
  - 密かに情報を埋め込む
  - 著作権情報などの保護に重要

情報を埋め込む

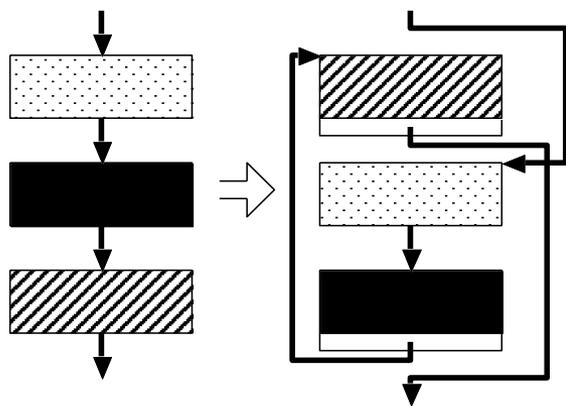


気づかれないように  
消えないように  
改変されないように



# 命令列表現の自由度

- 自由度  $f$  があれば情報  $\log_2 f$  (bit) を埋め込める
  - 等価な命令:  $\text{sub} (r \leftarrow r - 1)$  と  $\text{add} (r \leftarrow r + (-1))$
  - 基本ブロックのアドレス
  - 基本ブロック内の命令の順序
  - 大域変数のアドレス
  - 局所変数の (SP 相対) アドレス, レジスタ割り当て
  - などなど



(1) $ax := var1$	<del>↗</del>	(2) $dx := var2$
(2) $dx := var2$	<del>↘</del>	(1) $ax := var1$
(3) $ax := ax + dx$		(3) $ax := ax + dx$

(1) $ax := ax + bx$	<del>⬢</del>	(2) $dx := dx + cx$
(2) $dx := dx + cx$		(1) $ax := ax + bx$
(3) $ax := ax + dx$		(3) $ax := ax + dx$

# 組込み・制御システムへの応用

- PLC命令列(ソフトウェア)を論理回路(ハードウェア)に変換して実装するプロジェクト
- 八洲熱学(株)との共同研究(2003~2004年度)
  - 高速・小型・高秘匿性制御回路の開発
- 都市エリア産学官連携促進事業(一般型)



整列巻取機・試作1号機



FPGA制御デモ機

# 専用回路技術の制振制御への応用

- 制御モデルから専用回路を生成・評価(2009)

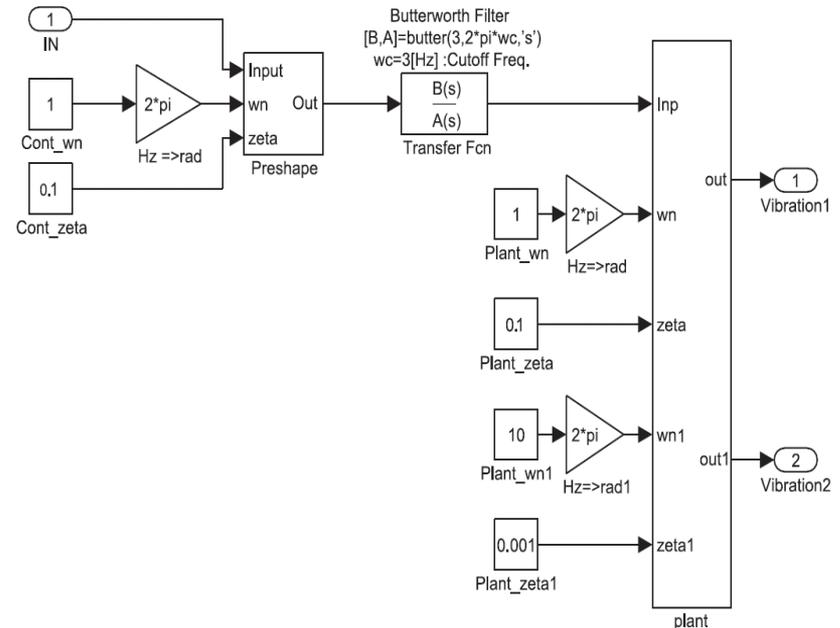
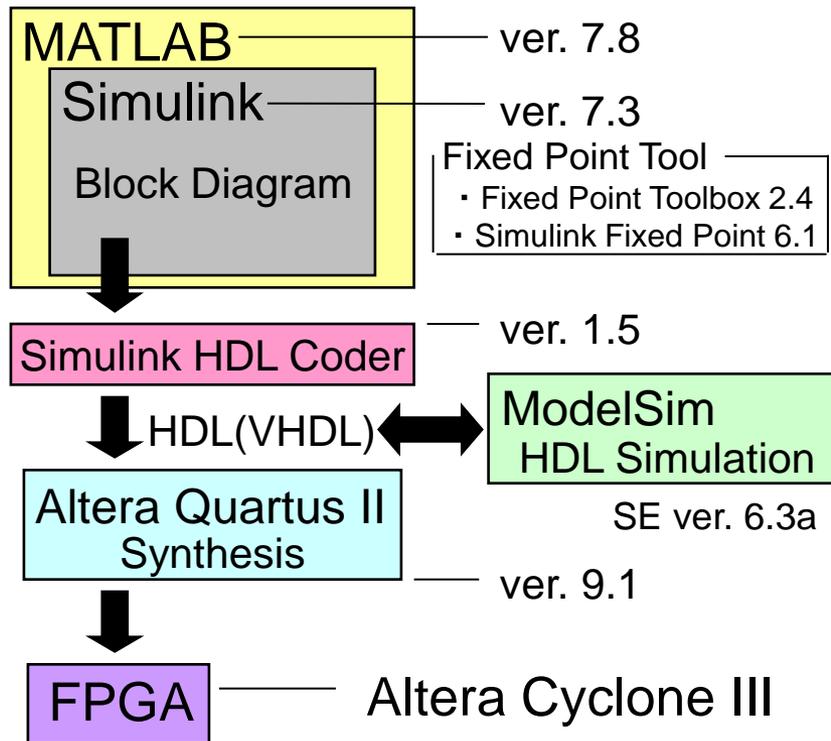


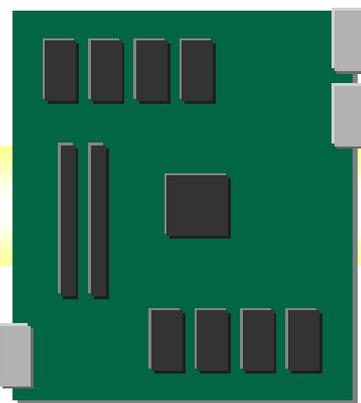
図6 ローパスフィルタ付き Preshaping Simulink モデル

# 組み込みシステムの性能測定と高速化

- 組み込みシステムにおけるCPUキャッシュに関する研究
  - (株)デンソーとの共同研究 (2007/9/1～2007/12/31)
  - 本テーマで卒業研究を行った学生は、実務訓練を共同研究先で行った



カーナビ筐体



組み込みシステム

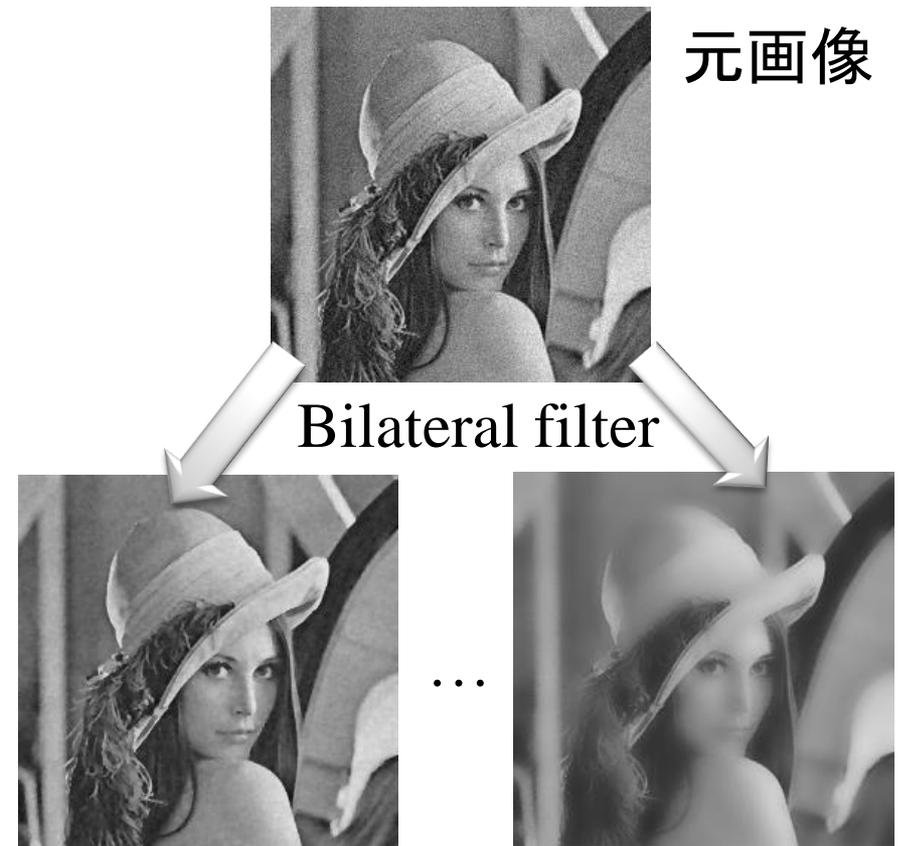


クロス開発環境

カーナビゲーションシステムの開発環境

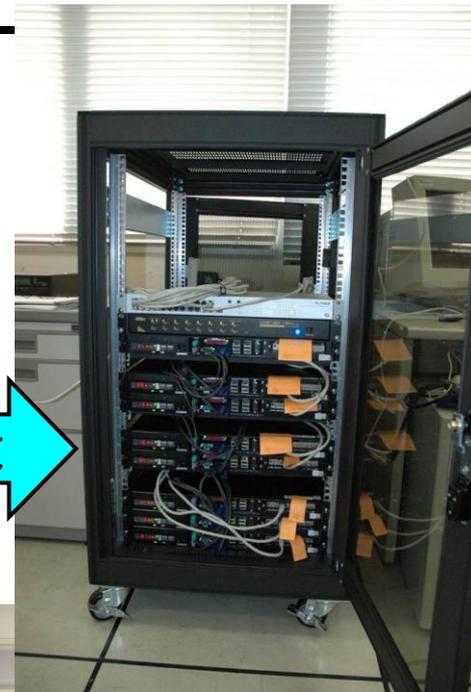
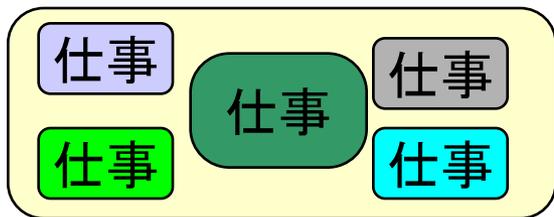
# 分布間距離を用いたBilateral Filter の準最適パラメータ探索

- Bilateral filterによるノイズ除去
  - 画像処理
- フィルタパラメータを適切に選択する必要がある
  - 最適パラメータの選択が難しい
  - 探索に多大な時間が必要
- 画質低下を抑えた準最適パラメータを短時間に探索する手法を提案



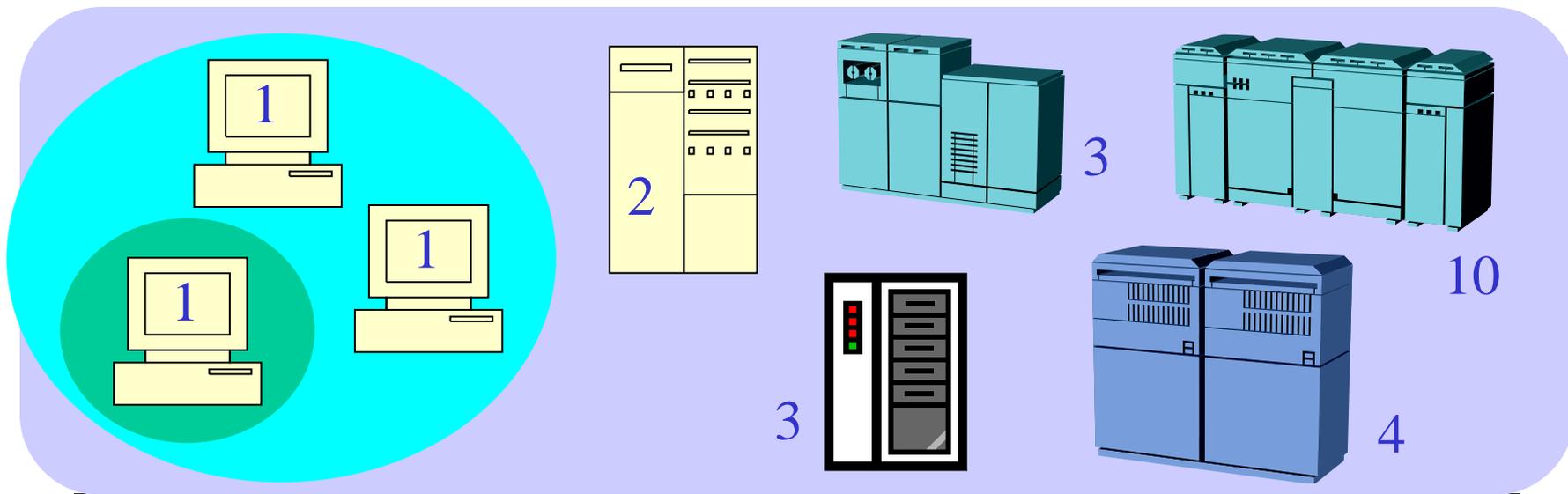
# 並列処理・分散処理の最適化

- ネットワークでつながった複数の計算機
  - PCクラスタ, 不均一なPCクラスタなど
- どうやって仕事を高速化するか？



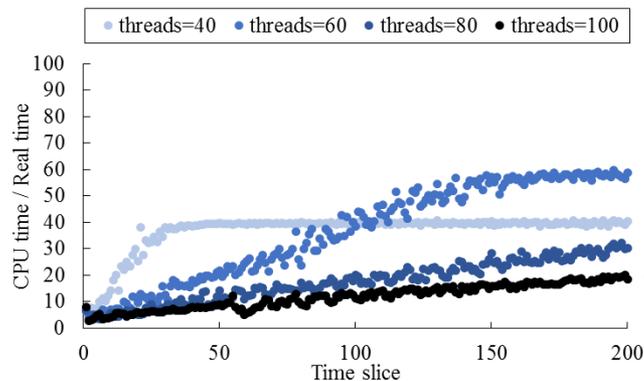
# 不均一クラスタ上での最適化

- 最適化 = 全体の実行時間を最小化する
  - 通信時間の考慮が重要
  - 各計算機に割り当てる最適な仕事量を求める
  - ワークロードに応じた最適な構成を求める
  - 実測に基づいた実行時間のモデル化 → 最適構成の予測



# メニーコアでの並列プログラム

- Xeon Phi: Intel のメニーコアプロセッサ
  - ワンチップで200スレッド以上の同時並列処理
  - 高並列・低通信なら高性能.....その他は??
- SAT(充足可能性問題)ソルバの性能評価(2017年度)
  - 高速化に向けた課題を明らかに



通信頻度が多すぎると、  
スレッド数を増やすほど性能悪化

# 卒業研究のテーマ（過去数年）

---

- 2024年度
  - FPGAによるSATアルゴリズムの検討
  - Staggered LFSRの回路設計と評価
  - ストカスティック数生成器の設計とFPGA実装
- 2023年度
  - 天文画像とLFSRによる乱数生成手法の検討
  - マルチリングプロセッサの設計
  - FPGA Implementation of the Staggered LFSR
- 2022年度
  - 気象データとLFSRを用いたURNGの改良
  - FPGA実装のためのオープンソースRISC-Vコアの比較
  - ストカスティック演算回路の合成
  - ソフトプロセッサCometにおける専用命令拡張方法
  - 並列SATソルバの比較と評価
- 2021年度
  - オープンソース高位合成ツールの調査と評価
  - ストカスティック数複製器の回路構成に関する検討
  - 気象データとLFSRによる乱数生成手法の検討
  - ソフトプロセッサCometにおける専用命令拡張方法の検討
- 2020年度
  - 超解像画像生成のためのBack Projectionハードウェアの高位合成
  - 単一ノード・マルチスレッド実行における Glucose syrupの性能測定
  - 内蔵 LFSR を利用した乱数生成手法の設計指針
  - オンライン乱数検定回路の高位合成に関する予備調査

# 修士論文のテーマ（過去の例）

---

- ・ セキュアハードウェア系
    - Obfuscator-LLVMとBambuを用いたハードウェア難読化
    - 高位合成によるLogic Locking手法の実装と評価
    - ハードウェア難読化のための難読化指標の検討
  - ・ 乱数生成回路系
    - マイクロプロセッサの内部状態とタイミング揺らぎを利用した乱数生成手法
    - 暗号資産価格の揺らぎとLFSRを利用した乱数生成手法
    - ラッチ型TRNGの軽量実装と乱数品質保持手法の検討
    - RSラッチのメタスタビリティを利用した真性乱数生成回路
  - ・ 専用回路系
    - 確率的計算を用いたGate Recurrent Unitの検討
    - Rocket-chipにおける専用命令の実装：乱数生成とストカスティック計算
    - 高位合成による専用命令実装手法の再評価
    - プロセッサの高位合成および特殊命令の実装・評価
    - 高基数モンゴメリ乗算法によるべき乗剰余演算の高速化
  - ・ 組み込みシステム系
    - 動的部分再構成を用いた耐故障化手法のXilinx Zynq-7000 SoCによる実装
    - PLC 命令列の高位合成によるハードウェア化と難読化
    - ハードウェア特殊化技術の制振制御への応用
    - 物体検出によるくずし字認識の検討
  - ・ 並列処理技術系
    - 分布間距離を用いたBilateral Filterの準最適パラメータ推定法における実行時間と推定精度のトレードオフ
    - 並列SATソルバによるXeon Phiの性能評価
-

# 各種情報

- 卒業論文・修士論文のテーマや, 各種研究情報はWWWで見ることができます

<http://www.ccs.ee.tut.ac.jp/ich/>



# 連絡先



- 教授 市川周一
- E-mail:  
ichikawa@tut.jp
- 住所: 441-8580  
豊橋市天伯町雲雀ヶ丘1-1  
豊橋技術科学大学  
電気・電子情報工学系