vlda 研究者各位

第 64 回「システム LSI 合同ゼミ」開催のお知らせ

発表時間制限のない自由な研究討論の場として，標記合同ゼミを下記のように企画いたしました．この合同ゼミは，不定期に開催される非公式の公開研究発表会で，1 研究室や 1 研究部署で行われている研究発表を複数の研究機関合同で行い，幅広く忌憚のない意見交換を行おうとするものです．ご興味のおありの方は是非お誘い合わせの上ご参加ください．

なお，本合同ゼミは年 3 回程度の割で，今後も引続き開催していく予定です．皆様からもご発表頂けるようでしたら，これほど嬉しいことはございません．ご遠慮無くご相談いただきたく，お待ち申し上げております．

金子峰雄（北陸先端科学技術大学院大学），
北澤仁志，藤吉邦洋（東京農工大学），
高島康裕（北九州市立大学），
小平行秀，富岡洋一（会津大学），
山田昭彦（コンピュータシステム＆メディア研究所），
梶谷洋司（設計アルゴリズム研究所），
貴家仁志（首都大学），
戸川望，史又華（早稲田大学），
築山修治（中央大学），
高橋篤司，岡田健一，原祐子（東京工業大学）
白石洋一，小林春夫 （群馬大学），

記

日時: 2016 年 10 月 29 日(土) 午後 1 時 30 分から午後 7 時頃まで（予定）
場所: 東京工業大学(大岡山キャンパス)
発表: 南 2 号館 2 階 S221 講義室 (午後 1 時 30 分より)
ポスター: 南 4 号館 2 階 S422 講義室 (午後 5 時 30 分頃より)
以下の URL をご参照下さい．
http://www.titech.ac.jp/maps/ookayama/campus/ookayama.html
30. 大岡山南 2 号館
32. 大岡山南 4 号館
ポスター懇談会: 午後 5 時半頃より同会場にて．

ポスター懇談会では，発表のあった研究に関してポスターボードを用いた研究討論を予定しております．軽食・アルコール飲料を準備いたします．ポスター懇談会のみの参加も歓迎します．

協賛: IEEE CEDA All Japan Joint Chapter

参加費: 1,000 円 (予定，当日払い)

申し込み: 合同ゼミ(ポスター懇談会のみも可)に参加ご希望の方は，準備の都合上，2016 年 10 月 25 日(火)までに，以下の連絡先までお申し込みください．

東京工業大学 高橋篤司
E-mail: atsushi@eda.ce.titech.ac.jp
Tel: 03-5734-2665/Fax: 03-5734-2902

【発表】

==========

(1) ２乗則を用いたデジタル乗算器アルゴリズムと FPGA 実装の検討

群馬大学大学院 理工学府 理工学専攻 電子情報・数理領域 小林研究室
博士前期課程２年 佐々木 秀

概要：デジタル乗算器はデジタル計算機、DSP チップ等に広く用いられているが、直接的に実現する と全加算器の２次元配列になり、回路規模・消費電力・演算時間が比較的大きくなってしまう。そのた め回路規模・消費電力の減少および高速化のために様々なアルゴリズムが提案され、それに基づきデジ タル乗算器が設計・実現されてきている。この論文では入力 A, B に対し その和と２乗から積 AB を 計算する式を用いてデジタル乗算器を設計する方式を検討した。また、そこで A, B のそれぞれの上位ビ ット、下位ビットに分割して計算量を低減する方式 (Divide & Conquer) を用いる。提案アルゴリズム を FPGA で実現・検証をすべく、検討したアルゴリズムで 8bit×8bit （出力：16bit），16bitx16bit (出 力 32bit)の乗算器を設計し RTL シミュレーションを行い、正しくデジタル乗算が行われていることを確 認し、FPGA 実装を検討した．提案方式で内部をパイプライン構成にすれば高速化が可能であり、小規模・高速のデジタル乗 算器を実現でき、一つのチップ内に多数配置でき大量のデータ処理が可能になる。

==========

(2) 逐次比較型時間デジタイザ回路の統計的手法による線形性自己校正技術の検討

群馬大学理工学部電子情報理工学科 小林研究室
学部 4 年 小澤祐喜

概要：時間デジタイザ回路は２つのクロック立ち上がりタイミング時間差をデジタル値として計測する回路である。その回路規模・消費電力を低減するため逐次比較型の構成を検討している。そこでは内部の遅延素子配列での遅延時間ばらつきにより時間デジタイザ回路の線形性が劣化する。そこで逐次比較時間デジタイザ回路に対して被測定信号が”電圧”ではなく”時間”であることを利用した統計的手法（ヒストグラム法を）によりその線形性劣化を校正する手法を検討した。本発表ではその原理・回路構成・シミュレーション結果およびその評価を報告する。検討手法はすべてデジタル回路で実現できるので、微細ＣＭＯＳ・ＦＰＧＡでの実現に適している。

==========

(3) 周辺回路を含む HMAC-SHA-256 回路に対するスキャンベース攻撃手法

早稲田大学大学院 基幹理工学研究科 情報理工・情報通信専攻 戸川研究室
修士 1 年 於久 太祐

概要：周辺回路を含む HMAC-SHA-256 回路に対するスキャンベース攻撃手法を提案する．入力メッセージから得られるスキャンデータを提案手法で解析することで，スキャンデータと HMAC-SHA-256 回路内のレジスタの対応関係を求め，メッセージ符号化に用いられた秘密鍵を復元する．計算機実験から，HMAC-SHA-256 回路とその他制御回路等のレジスタがスキャンチェインに接続されている場合でも，提案手法により回路全体のスキャンデータから HMAC-SHA-256 回路の内部レジスタの対応付けができ，メッセージ符号化で用いる秘密鍵を復元できることを確認した．

==========

(4) 単一命令セットコンピュータを用いたハードウェア故障検出手法

東京工業大学 大学院理工学研究科 通信情報工学専攻 原研究室
修士 2 年 張 栩生

概要：CMOS の微細化に伴い、ハードウェアの脆弱性が増え、故障によって誤動作するリスクが高まっている。耐故障化設計のためには、そのような故障の検出が重要な課題である。従来の多重化ベースの検出手法は回路面積のオーバヘッドが大きく、組込みシステムに適していない。本研究では単一命令セットコンピュータ(OISC)という小型プロセッサを用いることにより、組込みシステム向けプロセッサの故障を少ない回路オーバヘッドで検出する方法を実現する。OISC のチューニング完全性により、あらゆる計算の故障検査を行うことができるというメリットがある。本研究では、故障検出率、回路面積及び消費電力の点において、二重化設計および既存研究と比べ、提案手法の有用性を評価する。

==========

注意事項：

(1) 質問は発表の途中でも構いません．発表者を育てるという趣旨もありますので活発なご発言を期待します．

(2) 発表時間に制限がありません．従って，予定されていた発表が次回送りになる可能性があります．

(3) 発表には研究途中の未発表のものも含まれます．このようなことはないとは思いますが，アイディアの盗用は決してなさらないようにお願いします．
