第 53 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．

築山修治（中央大学），
金子峰雄，梶谷洋司（北陸先端科学技術大学院大学），
山田昭彦（CS メディア研），
貴家仁志（首都大学），
戸川望（早稲田大学），
高橋篤司，岡田健一（東京工業大学），
高島康裕（北九州市立大学），
小平行秀（会津大学），
北澤仁志，藤吉邦洋（東京農工大学）
白石洋一、小林春夫（群馬大学）

記

<<第 53 回システム LSI 合同ゼミ>>

日時： 2013 年 1 月 26 日(土) 午後 2 時から午後 7 時頃まで(予定)
場所： 東京農工大学 小金井キャンパス 11 号館 5 階 L1153 講義室
以下の URL をご参照下さい
http://www.tuat.ac.jp/basic_information/access/index.html#p3
ポスター懇談会: 午後 5 時頃から隣の L1151 講義室にて
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．

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，2013 年 1 月 22 日(火)までに，以下の連絡先までお申し込みください.
申し込み，ご質問等宛先： 東京農工大学 藤吉邦洋
E-mail: fujiyosi@cc.tuat.ac.jp
Tel/Fax: 042-388-7250
==========

発表：

(1) 信号成分なしフィードバック（Signal-nulled Feedback）低雑音増幅器の雑音解析
群馬大学大学院 工学研究科 電気電子工学専攻 博士前期課程 1 年 興 大樹

広帯域低雑音増幅器（Low Noise Amplifier: LNA)の低雑音化技術として
信号成分のないフィードバック低雑音増幅回路（Signal-nulled Feedback
LNA）の原理と雑音低減効果のシミュレーション検証を示す。
この回路は出力の位相が反転するメインアンプと、
メインとサブアンプ両方の MOSFET のチャネル雑音低減するサブアンプを含む
負帰還ループにより構成される。
負帰還ループではメインアンプの入出力を用いて
信号成分をキャンセルし（Signal-Nulled)、サブアンプに入力する。
負帰還ループで発生する消費電力を抑えつつ低雑音化を実現することができる。

(2) 排他的制御を用いた単一インダクタ 2 出力 DC-DC スイッチング電源
群馬大学大学院 工学研究科 電気電子工学専攻 博士前期課程 1 年 李 慕容

環境問題への関心への高まり等から電源回路技術への要求がますます
厳しくなってきている。その社会的・産業的な要求に応えるため、
低コスト化・小型化のために部品点数を減らして複数電源出力を得るための、
排他的制御を用いた単一 インダクタ 2 出力 DC-DC スイッチング電源を提案し、
その原理、回路構成、シミュレーション結果を示す。

(3) Trivium へのスキャンベース攻撃におけるビット対応解析手法

早稲田大学 基幹理工学部 情報理工学科 戸川研究室 学部 4 年 藤代美佳

ストリーム暗号へのスキャンベース攻撃では，スキャンチェインを用いて回路内部の状態を取得し，取得した内部情報を元にキーストリームと平文を復元する．ストリーム暗号 Trivium への従来の攻撃手法は，暗号回路の内部レジスタのみがスキャンチェインに含まれていることが前提であり，周辺回路のレジスタがスキャンチェインに含まれている場合，スキャンチェインの内部構造を解析できない．一般に，LSI チップ上の他の複数の回路が同一スキャンチェインに含まれることはあるため，実際の攻撃手法としての利用は難しい．本発表ではスキャンチェインの構造に依存しない手法を提案する．提案手法をソフトウェアでシミュレーションし，周辺回路を含むスキャンチェインでも解析可能なこと，従来手法より効率的に解析できることを確認した