「ディペンダブル VLSI システムの基盤技術」
平成 20 年度採択研究代表者

H24 年度
実績報告

吉本　雅彦

神戸大学　大学院システム情報学研究科・教授

超高信頼性 VLSI システムのためのディペンダブルメモリ技術

§1. 研究の概要

1. 1 チーム全体の研究の概要

(1) 本研究の背景と課題定義

現在、情報通信・コンピュータ・交通などの重要な社会インフラはシリコン LSI によって支えられている。しかしながら微細化・大規模化・高性能化が進む LSI では、放射線によるソフトエラーやトランジスタが時間的に劣化する NBTI (negative bias temperature instability)などの物理的エラーによる信頼性低下が問題となっている。加えて、あまりに複雑化した LSI 設計やその製造・検査段階において発生する人為的エラーを完全には排除できない状況となっている。このことは製品がエラーを持ったまま出荷され、さらに偶発的なエラーも加わることを意味しており、もはや完璧に信頼できる LSI は望めない。速度・電圧・温度・入出力信号の品質などの想定される外部環境のあらゆる組み合わせにおいて、満足して動作することは不可能であり、信頼性の低下があってもそれを改善できる機構を持った LSI が望まれている。これがディペンダブル LSI である。

本研究ではディペンダブルなメモリ技術に着目する。システム LSI においてはメモリ SRAM の大容量化が進み、現在では総トランジスタ数の 90%以上を占めるに至っている。そのため、LSI のディペンダビリティは組み込み SRAM が支配すると言っても過言ではない。ＳＲＡＭのディペンダビリティを阻害する要因として、次の６項目が挙げられる。素子の経年劣化、電源ノイズなどの電圧変動、温度変動、ソフトエラー、サイドチャネルアタック、不正アクセスである。

そこで、本研究では、上記６項目への対策技術開発を課題とする。すなわち、マージン不良を出さない設計技術、不良予知診断技術、不良回避技術、統合化プラットフォーム技術、統合試作による検証、システムレベル検証技術の６つの側面から設計技術を研究する。これらの課題を解決することで、ｉ）不良予知、検出、回避までの一貫したＳＲＡＭの信頼性向上のためのディペンダビリティメモリ技術開発を行うとともに、それを SoC 設計に発展させ、ディペンダブル SoC プラットフォーム技術開発を実施する。

(2) 本研究の特徴

本チームによる研究の最大の特徴は、自律型ディペンダブルメモリ開発だけでなく、その最終応用におけるシステム信頼性を評価できるチーム構成を確立していることにある。そのため、ディペンダブル VLSI の重要な応用である特に車載制御システム信頼性向上効果の定量的検証を可能としている。

(3) 本研究の達成目標

① 第1の目標は、自律型ディペンダブルメモリの開発。これにより、トランジスタ特性の経年劣化、環境変動（雑音等による電圧変動、温度変動）によるSRAM動作マージンが劣化しても自律的にマージンを改善し動作を継続できるメモリシステムを構築する。
② 第2の目標は、上記SoCﾌﾟﾗｯﾄﾌｫｰﾑ技術を用いた EV 向け EMI 対策技術とメモリベースセキュリティ技術を開発する。
③ 第3の目標は、前期要素技術を統合的に適用したディペンダブルメモリベース・マルチコアSoCアーキテクチャの開発。
④ 第4の目標は、メモリへの不良注入技術（新規開発）を導入した Virtualization 技術（PILS: Processor-In

the Loop Simulation）の構築とディペンダブルメモリによる車載制御システム信頼性向上効果の定量的検証。

1．2 研究実施方法

（1） 本研究チーム全体の運営と取りまとめ方針

メモリという最もデバイスに近い技術であるが、回路技術、SoCアーキテクチャ、想定応用システム（車載制御）まで縦に通した垂直統合研究を実施する。

（2）研究グループの分担

① 「吉本」グループ（研究代表者グループ）

・耐ソフトエラー技術を開発する。SRAM の宇宙線による誤動作対策として従来技術として ECC があるが速度性能を劣化させる。またマルチプアップセットでは ECC は有効ではない。そこで、メモリセルレイアウトに改善を加えてマルチプルアップセットを低減する。

目標：宇宙線によるマルチプルアップセットを1桁低減する。

・不良回避技術として、新規提案の QoB (Quality of Bit)メモリ技術（回避方式1）を開発し、自律型ディペンダブルメモリシステム（自律的に不良を予知し不良回避できるキャッシュメモリ）を開発する。内蔵 BIST とオンチップ・電圧モニターによりウェイ数可変キャッシュを制御することで FIT 値を改善する。

目標：電源ドループ雑音印加時の FIT 値を2桁改善する。

・自律型ディペンダブルメモリのマルチコアアーキテクチャへの適用技術を開発する。特に、QoB メモリをメモリ LockStep 機構に適用する。QoB メモリの一括比較機能、一括コピー機能をワークメモリ、ワーキングレジスタに活用し、高速なチェックポイント・リカバリを実現すr。

目標：DMR における性能オーバヘッドを最小限に抑えながら、システムエラーレートの 2 ケタ改善, MTBF・MTTR・Availability の改善の実証を目指す。

② 「永田」グループ（共同研究第1G）

・チップ内電圧モニタリングによる不良予知診断技術

VLSI システムに搭載された SRAM に関して、とりわけ VLSI チップの実装システムが外部から受ける電磁ノイズが、SRAM の動作に作用しビット不良を引き起こす。この過程の物理的なメカニズムを解明するとともに不良を予知する診断技術を開発し、動的な電源ノイズに対するディペンダビリティを実現する。

課題： SRAM の電磁ノイズ耐性を評価する実験手法を確立し、メカニズムを解明する。このために、(1) 本研究グループに実績のあるオンチップ電圧モニタ(OCM)を用いた電源ノイズの観測技術、(2)IC チップにおける電磁ノイズ耐性の評価手段として EMC 分野で標準化されている RF 電力注入試験法(DPI)、および(3)VLSI テスト分野の技術である埋め込みテスト技法(BIST)、の三者を組み合わせる。

目標：前記の観測的知見を得るとともに、SRAM の不良予知診断手法を確立する。

・EV 向け EMI 対策のための電源ノイズフィルタの開発（H23 年度までは「耐タンパ性拡張フレキシブル電源ネットワークの開発」として取り組み）

VLSI システムにおける電源ノイズの発生および電磁ノイズに対する耐性は、VLSI 搭載機器における電源供給系のインピーダンス特性に強く依存する。普及の進む EV・PHV に着目し、EV 向け EMI 対策として、車載電子機器における VLSI の電磁環境に対するディペンダビリティを実現する。

課題：電源ノイズを効果的にフィルタリングする電源ネットワークの設計手法を開発する。このために、本研究グループに研究実績のある、LSI チップ-パッケージ-ボードを統合した電源ノイズのモデル化およびシミュレーション技法を活用する。

目標：(1)オンチップとオフチップの回路要素を統合した電源ノイズフィルタの設計法を確立すること、および(2)フィルタの効果を車載環境で評価可能とするオンチップ電圧モニタ技術を開発すること、を目標とする。

③ 「新居」グループ（共同研究第2G）

・フレキシブル電源ネットワーク技術、細粒度電圧制御による SRAM の不良回避技術

細粒度動的電圧制御（回避方式２）による不良回避技術を実施する。課題：出荷後フィールドでのメモリ故障・電圧マージン劣化でシステム機能安全性が低下してしまう。リード不良回避方法（ワード線低下回路）、ライトマージン不良回避方法（セルバイアス降下回路、負ビット線バイアス回路など）を採用し、不良予知技術と組み合わせる。目標：それらの改善効果として 100mV の動作下限

電圧改善を図ること。

・メモリベースID/暗号鍵生成技術の開発

SRAM のランダムビット不良を利用した固有 ID の生成、暗号鍵生成および認証によるセキュリティ機構を開発する。課題：一意性と再現性を高めること。特にプロセス・温度・電圧変動に対して安定的に固有 ID を生成することが重要である。目標：電源電圧変動±１０％、-40℃～125℃の温度変化の環境下でも安定して固有 ID を生成できることを実デバイスにて実証する。

④ 「勝」グループ（共同研究第3G）

・故障注入 CPU モデルベースのハードウェア/ソフトウェア協調シミュレーション(Virtualization)

課題：開発効率の向上のために、実物を用いずに性能検証が可能なシミュレーション技術の開発

目標：ソフトウェア動作時のメモリ故障解析が可能なオールシミュレーション検証環境の構築

・マルチコアプロセッサ向け Virtualization の技術開発

課題：現状実在しないハードウェアアーキテクチャに対してモデルを用いたシミュレーションによる性能評価を可能にする

目標：代表者 G が開発する自律型ディペンダブルメモリのマルチコアアーキテクチャ性能評価環境の構築

⑤ 「於保」グループ（共同研究第4G）

本研究成果の自動車向け出口戦略を策定するため、産業界の動向を調査研究する。CREST の性格上、本研究では先導的な技術を多々取り扱っている。これが産業界のニーズに照らして妥当であるかを検証するとともに、産業界に対し本研究の成果を提示し、その受容性を探る。このため試作デモを含めて本研究成果の有効な自動車応用を具体化する。

（3）領域外部の企業等との連携

研究チームには、ルネサスエレクトロニクスが参画しており、半導体メーカとの直接的な共同研究体制にある。また、Virtualization を担当する共研3G（日立中研）は車載機器メーカと密な連携関係を持っており、本研究成果を実応用システム（車載応用）で検証できる環境にある。また、Virtualization では、EDAベンダの Synopsys 社と連携して、IPコアの開発を進めている。

（4）領域内他研究チームとの連携関係

安浦チームと連携して、ソフトエラーレート（SER）予測技術とSER改善技術の研究に取り組んでいる。特に、物理、デバイス、回路、アーキテクチャの垂直統合シミュレーションによる評価方法の確立に取り組んでいる。

また、「チップ内電圧モニタリングによる不良予知診断技術」および「耐タンパ性拡張フレキシブル電源ネットワークの開発」に関して、研究チーム内ではルネサスエレクトロニクスグループ（共研2G）と永田グループ（共研1G）で密接に連携しており、いずれのトピックについても、VLSI システム製品の将来において必要となる機能や仕様について意識共有を図りながら研究を実施している。

1．3　研究グループの今年度の研究の狙い

① 「吉本」グループ（研究代表者グループ）

・自律型ディペンダブルメモリによる不良回避技術の評価

統合試作により開発された自律型ディペンダブルメモリ（256KB/8Waキャッシュ）の電源電圧ノイズ耐性を評価する。特に、低周波電源ドループ印加時の耐性について、ドループの深さおよびドループの長さをパラメータとして評価し、自律型ディペンダブルメモリの有効性を実証する。

・ディペンダブルメモリを応用したマルチコアプロセッサアーキテクチャ

自律型ディペンダブルメモリ（不良予知技術および不良回避技術）をマルチコアプロセッサのディペンダビリティ向上に有効に役立たせる技術を開発する。特に、QoB の一括コピー機能、一括比較機能、および細粒度 QoB キャッシュメモリと細粒度電圧制御技術を組み合わせ、ディペンダブルマルチコアプロセッサにおける性能オーバヘッドを最小限に抑えるアーキテクチャを開発し、従来

技術（シングルコア密結合型、ロックステップマルチコアマイコン）に対する優位性を明確にする。

② 「永田」グループ

・チップ内電圧モニタリングによる不良予知診断技術

平成 24 年度は、SRAM における電源ノイズ感度の支配要因を明確にし、平成 23 年度に試作した統合試作チップにおける SRAM の不良予知の条件を定めることを狙いとした。このために、OCM、DPI、BIST の三者を組み合わせた SRAM のノイズ感度評価システムの完成度を高め、動作周波数、ノイズ周波数、相互タイミング（位相差）、およびノイズ振幅に着目し、これらの物理パラメータに対する SRAM 不良ビット発生率の感度特性を詳細に評価することとした。

・EV 向け EMI 対策のための電源ノイズフィルタの開発（H23 年度までは「耐タンパ性拡張フレキシブル電源ネットワークの開発」として取り組み）

平成 24 年度は、電源ノイズフィルタの設計に用いる「LSI チップ-パッケージ-ボードを統合した電源ノイズのモデルリング手法」について、広い周波数範囲における電源ノイズの解析性能を向上することを狙いとした。また、車載環境における VLSI チップのノイズを観測するため、実験室系のような広域の電圧基準（グラウンド）を持たない評価環境、すなわち車載環境や屋外環境におけるオンチップ電圧モニタ機構の動作を確立すること、を狙いとした。これらの目的のため、前年度までに試作したノイズ発生の評価チップおよびノイズフィルタのための要素回路チップにおけるノイズ特性を、実験と解析の両面から詳細に評価することとした。

③ 「新居」グループ

・自律型ディペンダブルメモリ LSI の評価・実機デモ

フレキシブル電源ネットワーク(FPSN)と細粒度アシスト SRAM、フィールド BIST、オンチップモニタを組み合わせた自律型ディペンダブルメモリ LSI(統合試作)を評価及び実機デモを行う。FPSN とフィールド BIST、オンチップモニタを1チップに統合し、細粒度アシスト SRAM、FPSN による不良回避を行う自律型ディペンダブルメモリを構成する。統合試作チップの評価を完了し、実機ボードによるデモ環境を構築する。

・SRAM のランダムビット不良を利用したチップ ID 生成機構によるメモリベースセキュリティ技術の開発

SRAM のランダムビット不良を利用したチップ ID 生成機構、暗号鍵生成および暗号鍵認証による耐タンパメモリベースセキュリティ技術を開発する。チップ ID 生成では、課題となるプロセス・温度・電圧変動に対して安定的に固有 ID を生成する回路技術を提案し、特許出願を行う。また、同じ SRAM モジュールを用いて、暗号鍵の生成および認証ができる耐タンパメモリ機構も開発する。本年度は、具体的に 40nm プロセスを用いたチップ ID 生成モジュールと暗号鍵生成・認証モジュールの設計を行う。そして、これらのモジュールを盛り込んだテストチップの設計・試作を行い、メモリベースセキュリティ技術の開発を行う。

④ 「勝」グループ

・マルチコアプロセッサ向け Virtualization の技術開発

不良回避技術（QoB・SRAM など）をマルチコアプロセッサに実装した際の評価に向けた、自動車制御システム上での検証環境構築を実施する。Virtualization 技術により、実機試作前に、開発アーキテクチャおよび回路技術の有効性を定量的に検証することが可能となる。今年度は、デュアルコアプロセッサにターゲットを絞り、QoB メモリの一括コピー機能、一括比較技術に関して Virtualization するために、コア間のレジスタ比較機構及びメモリ比較機構のモデル化を実施する。

⑤「於保」グループ

本研究の主要な成果の一つである SRAM の故障注入を一般化し、自動車制御ユニット（ECU）の故障注入解析技術として産業界に提示して、本技術の受容性を探る。ECU の品質保証では FMEA (Failure Mode and Effect Analysis)手法が広く使われている。しかし従来の FMEA では LSI 内部の部分故障、あるいは一次故障を想定していない。本研究の Virtualization 技術はこれらのシミュレーション解析を可能とするものであり、この技術に対する産業界の反応を探る。

§2. 研究実施体制

①「吉本」グループ
ア 研究分担グループ長: 吉本 雅彦(神戸大学大学院システム情報学研究科、教授)(研究代表者)
イ 研究項目
・マージン不良最少化技術として、耐ソフトエラー技術の開発
・フィールドでのチップ内加速試験による不良予知診断技術の開発
・ＱｏＢ・ＲＡＭを用いた不良回避技術の開発。
・統合技術による自律型ディペンダブルメモリシステムの開発
・ディペンダブルメモリベース・マルチコアアーキテクチャの開発

②「永田」グループ
ア 研究分担グループ長: 永田 真(神戸大学大学院システム情報学研究科、教授)
イ 研究項目
・ 不良予知診断による預錯設計技術
・ SRAM 動作環境モニタの開発と評価
・ SRAM ビットエラー予測システムの構築
・ 電源ノイズの評価
・ LSI チップ-パッケージ-ボードを統合した電源ノイズ解析手法の確立

③「新居」グループ
ア 研究分担グループ長: 新居 浩二(ルネサスエレクトロニクス、設計基盤開発統括部、課長)
イ 研究項目
・ 細粒度電圧制御によるメモリ不良回避技術の開発
・ ディペンダブルメモリシステムのハードウエアプラットフォームの開発
・ SRAM のランダムビット不良を利用する ID 生成技術の開発

④「勝」グループ
ア 研究分担グループ長: 勝 康夫(日立製作所、中央研究所、主任研究員)
イ 研究項目
・システムレベル検証技術の開発と車載応用への適用

⑤「於保」グループ
ア 研究分担グループ長: 於保 茂(日本工業大学、教授)
イ 研究項目
・自動車向け出口戦略の調査研究

§3. 研究実施内容

(文中に番号がある場合は(4－1)に対応する)

3. 1 研究の成果と自己評価

(1) 成果1.「LSI チップ-パッケージ-ボード統合ノイズシミュレーションの高精度化」(永田グループ)

①内容　電源電流モデルと電源ネットワークモデルの統合により、32 ビット・マイクロプロセッサの動作時における電源ノイズについて、広い周波数範囲かつベクタ時間長にわたるノイズ波形のシミュレーションを実現した。[12]

図 1-1 に示すように、デジタル LSI の電源電流モデルについては研究グループが独自に提案している充電容量モデルを拡張し、また電源ネットワークモデルについては、LSI チップ、パッケージ、ボードの電源インピーダンスの構成要素を集中定数あるいは分布定数的に抽出して構築している。

32 ビット・マイクロプロセッサが 10 MHz の低速動作をしている時の電源ノイズについて、実測とシミュレーションによるノイズ波形と周波数成分を図 1-2 に比較している。低速動作ではクロックエッジ直後のリンギングが顕著であり、LSI チップ、パッケージ、ボード、の統合ネットワークにおける共振特性が主因と考えられる。波形の形状や振幅、および周波数成分について、シミュレーションと実験の良い一致が得られている。また、プロセッサの動作プログラムからオペコードおよびオペランドが変遷しているときのノイズ波形を図 1-3 に示している。長大なクロックサイクル数の時間幅に対してノイズ波形が精度よく解析されており、プロセッサの動作内容に応じたノイズ振幅の発生が表現されている。

②有用性　「LSI チップ-パッケージ-ボードを統合した電源ノイズのモデルリング手法」を確立し、広い周波数範囲かつさまざまなプログラムに対して電源ノイズの解析が可能である。EV 向け EMI 対策のための電源ノイズフィルタの開発においては、車内の電磁場環境に影響の大きい、電力系統の低周波数ノイズから情報通信系の高周波数ノイズをカバーするノイズ解析の実現に役立つ。また、ノイズ発生のシミュレーションモデルは、外来ノイズの逆伝搬(イミュニティ)特性の解析にも有効である。

③優位比較　LSI チップ-パッケージ-ボード(LPB)の統合解析・設計について、日本国内でも JEITA の LPB 相互設計ワーキンググループを中心として実務的なフローの開発が進んでいる。しかしながら、VLSI チップの実測データとの整合を含めた LPB 統合シミュレーション精度評価は報告されていないと思われ、本技術は補完的に活用できるものと考えられる。

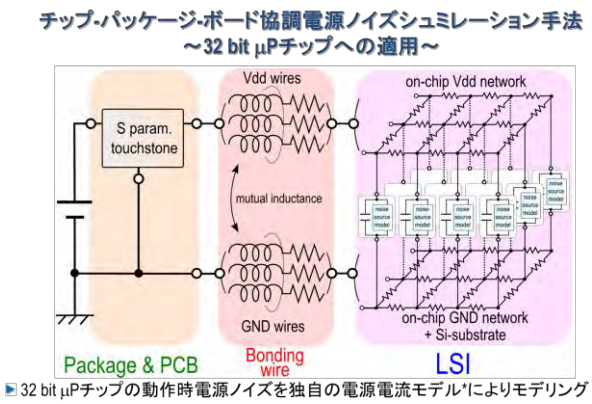


図 1－1

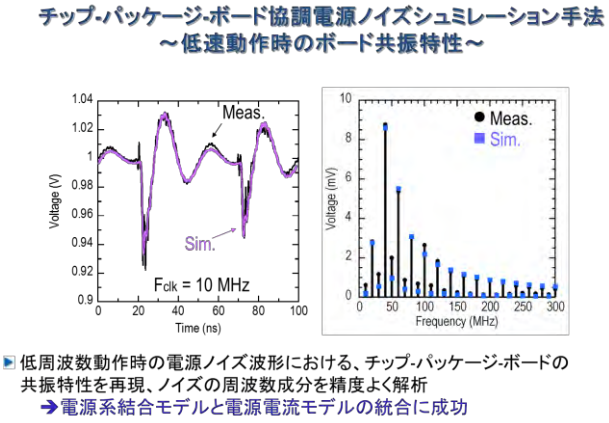
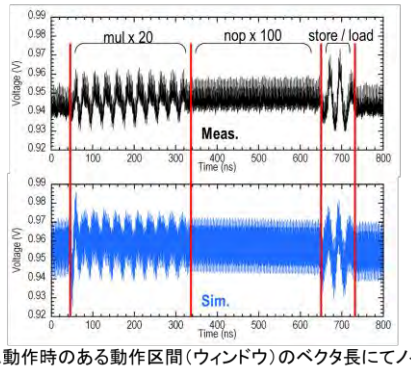


図 1－2

チップ-パッケージ-ボード協調電源ノイズシュミレーション手法
～長い動作時間のノイズ波形を解析～



▶プログラム動作時のある動作区間（ウィンドウ）のベクタ長にてノイズ波形を解析

図 1－3

（2） 成果2.「可搬型オンチップ電源モニタのデモンストレータの開発」（永田グループ）

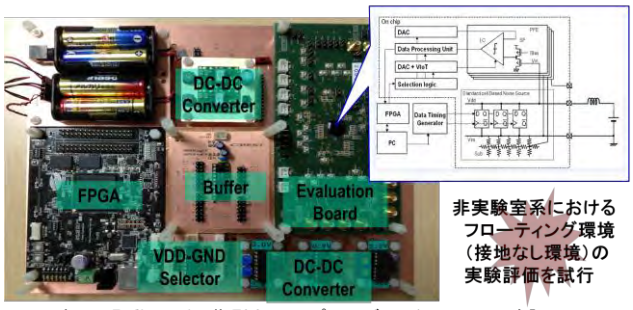
①内容　オンチップ電源モニタによるLSIチップのノイズ評価系を電池駆動化し、小型で可搬としたノイズ評価のデモンストレータを開発した。[10]

図 2-1 に示すように、テストチップ、信号発生要素、および各種の電源回路、および電池を小型の基板上に実装した。テストチップに搭載したデジタル回路の動作時における電源ノイズについて、図 2-2 のように波形として取得するデモンストレーションを可能とした。ここで、電源ノイズは(i)デジタル回路内部の電源配線(Vdd)、(ii)デジタル回路内部のグラウンド配線(Vss)、および(iii)デジタル回路内部の電源-グラウンド間の実効電圧(Veff)、として測定される。これらに加えて、実効電圧そのものを検出する新しいオンチップ実効電源モニタ回路も評価した。図 2-2 には、前項の(i)(ii)による計算値 Veff=Vdd-Vss と(iii)による Veff の測定値が良く一致することもあわせて示している。テストチップには、前年度までに試作したノイズ発生の評価チップおよびノイズフィルタのための要素チップを活用した。

②有用性　EV 向け EMI 対策のための電源ノイズフィルタの開発において、車載環境における VLSI チップ動作時ノイズのオンチップ評価を実現するためのオンチップ電源モニタの機能と性能の拡張が求められる。本デモシステムは、実験室系のような広域の電圧基準（グラウンド）を持たない評価環境、すなわち車載環境や屋外環境におけるオンチップ電圧モニタ機構の動作の確立に活用できる。

③優位比較　本デモシステムは、回路技術の国際会議：IEEE Asian Solid-State Circuits Conference 2013 において一般公開した。LSI チップの内部ノイズ波形をその場で観測する事例はこれまでに無く、多くの聴衆から関心を得た。オンチップ電源モニタ技術は国内外の半導体メーカからも報告例があるが、その場でデモンストレーションできる評価システムとしては実装されておらず、本研究の成果が研究開発における利用性の高さにおいて有意性が高いと考えられる。

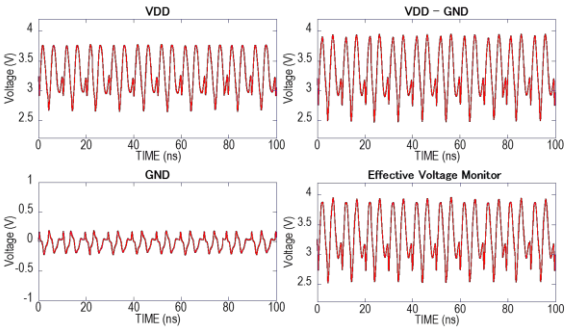
オンチップ電源モニタの拡張
~ODMによる電源ノイズ測定システムの可搬化~



▶フルバッテリ駆動による可搬型オンチップ・ノイズモニタシステムの実証
➔ 車載や屋外環境におけるVLSIチップのノイズ観測に向けた第一歩

図2－1

オンチップ電源モニタの拡張
~可搬型ノイズ評価システムによる波形取得例~



▶デジタル回路の電源(Vdd)、グラウンド(Vss)、実効電圧(Vdd-Vss)の波形を取得
（あわせて、実効電源電圧モニタによる測定波形との一致性も確認）

図2－2

(3) 成果3.「自律型ディペンダブルメモリ LSI の評価・実機デモ」(新居グループ)

①内容

フレキシブル電源ネットワーク(FPSN)と細粒度アシスト SRAM、フィールド BIST、オンチップモニタを組み合わせた自律型ディペンダブルメモリ LSI(統合試作)を開発。FPSN とフィールド BIST、オンチップモニタを1チップに統合し、細粒度アシスト SRAM、FPSN による不良回避を行う自律型ディペンダブルメモリを構成する。統合試作チップの SRAM 評価を完了し(図 3-1、3-2)、実機ボードによるデモ環境を構築、動作確認を行った。(図 3-3(試作チップのブロック図)、図 3-4(試作チップのレイアウトプロット)、図 3-5(デモ環境))

②有用性

近年、自動車用途の MCU では自動車用機能安全規格 ISO26262 への対応が強く要求されている。自律型ディペンダブルメモリシステムは、システム動作を妨げることなく、不良検知および不良回避をバックグラウンドで自律的に行える。

③優位比較

従来 SRAM のエラー検出は ECC に
テムでは、電圧も含めた動作マージン
作のバックグラウンドで自律的に行な
る。

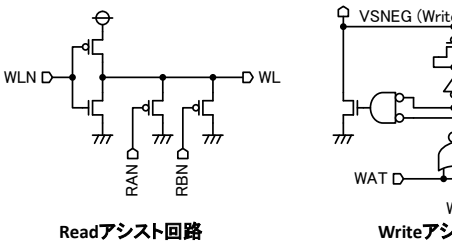


図 3-1 細粒度アシスト回路

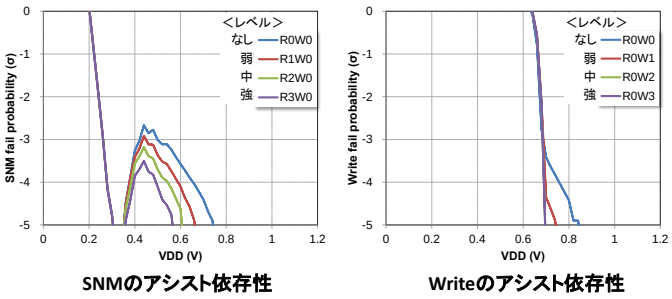


図 3-2 実測結果

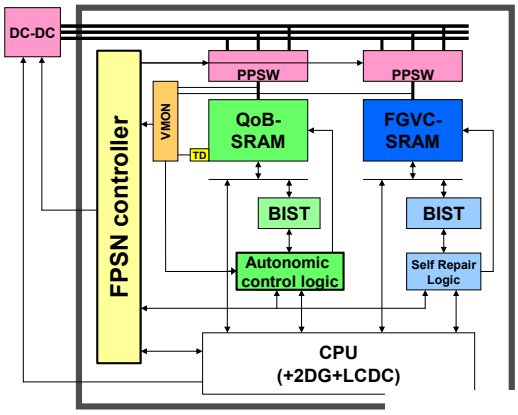


図 3-3 試作チップのブ

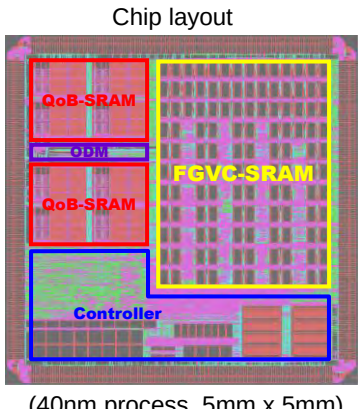


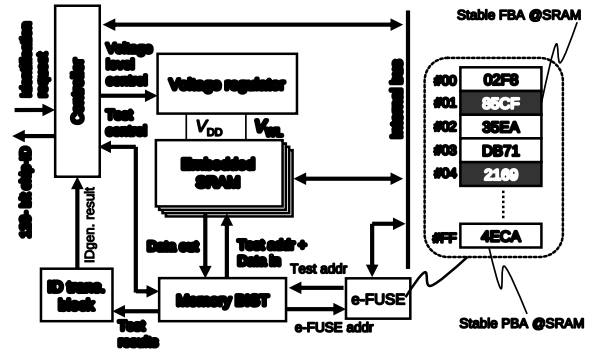
図 3-5 デモンストレーション環境

(4) 成果4.「SRAM のランダムビット不良を利用したチップ ID 生成機構によるメモリベースセキュリティ技術の開発」(新居グループ)

①内容

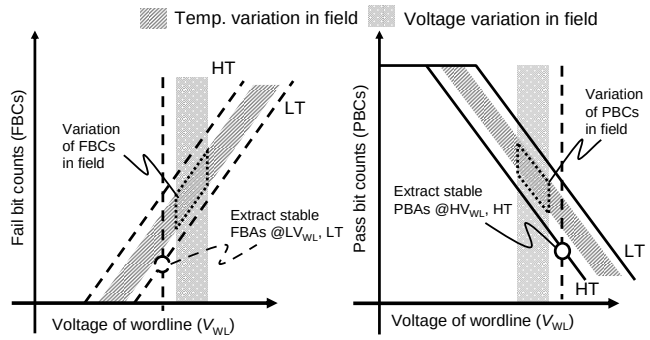
次に、発展テーマの1つであるチップID生成について報告する。図 4-1 は、SRAMのランダム不良を用いたチップID生成機能の再現性を高めたブロック構成図を示す。チップID生成時にアシスト回路のバイアス条件を不良が発生しやすくなるように逆方向に制御(ワード線電位を昇圧)し、その不良アドレスをチップIDに用いる。

課題であった温度変化、電圧変動に対するID生成の再現性を高めるために、製品出荷前にあらかじめ必ずPass もしくは Fail するアドレスを取得し、Fuse 等の不揮発素子に記憶させておく(Pass/Fail が不安定なアドレスを除くスクリーニングテストを実施する)。実使用時(ID 生成時)には不揮発素子に記憶してあるアドレス(安定して Pass もしくは Fail するアドレス)に対して MBIST を用いてテストを実施し、テスト結果が不良となるアドレスのみから、ID の生成を行う(図 4-1)。また、Pass アドレスからは ID が生成されない(Pass アドレスは耐タンパ性の観点から偽のアドレスとして扱う)。



•必ずPass/Failするアドレスをe-FUSE等の不揮発素子に記憶。

図 4-1

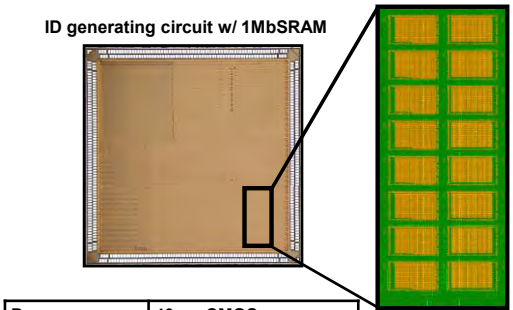


安定FBA(Fail-bit-address): PVT-Best(不良が発生しにくい)条件で取得
安定PBA(Pass-bit-address):PVT-Worst(不良が発生しやすい)条件で取得

図 4-2

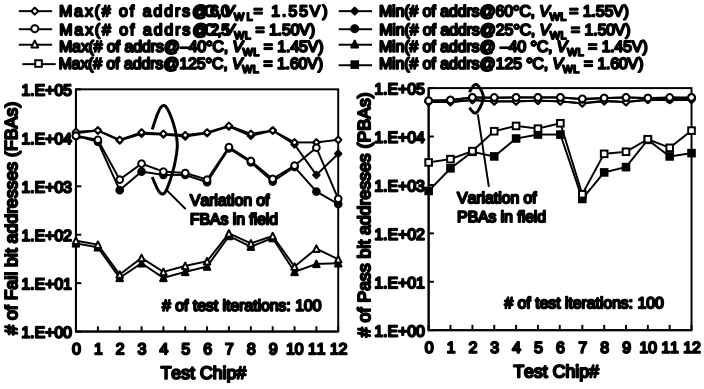
スクリーニングテストの方法を図 4-2 に示す。安定した不良アドレスを取得する場合、出荷前のテスト条件を実使用条件よりも不良が“発生しにくい”条件(低ワード線電位、低温)に設定する。こうすることにより、出荷前テストで取得された不良アドレスは実使用時において、必ず不良となる。同様に、安定したパスアドレスを取得する場合は、テスト条件よりも不良が“発生しやすい”条件(高ワード線電圧、高温)に設定する。これら2つの手法を用いることによって、安定して Pass もしくは Fail するアドレスを不揮発素子に書き込み・記憶することが可能となる。

図 4-3 に 40nm プロセスを用いて試作を行ったチップ写真を示す。図 4-4 にスクリーニングテストの実測結果を示す。実使用を想定した条件(ワード線電圧(Vwl):1.5～1.55V、温度:25℃～60℃)における不良アドレス(FBA)の個数は、スクリーニングテストの条件(Vwl: 1.45V、温度:－40℃)における不良アドレスの個数よりも常に大きくなっている。さらに、スクリーニングテストの条件で発生した全ての不良アドレスが、実使用の条件で発生した不良アドレスに含まれるという結果も確認済みである。パスアドレス(PBA)についても、同様の結果を取得することができた。



Process	40nm CMOS
SRAM capacity	1Mb
Area overhead	8.1-k gates
ID gen. time	< 10us @ 200MHz

図 4-3



FBA@Field⊇FBA@Test & PBA@Field⊇PBA@Test
になることを確認

図 4-4

以上から、提案するスクリーニング手法を用いることにより、温度変化、電圧変動に対するID生成の再現性の向上が可能であるということを確認することができた。

②有用性

近年の SoC では少なくとも数 Mbit 規模のオンチップ SRAM とそれをテストする BIST 機能が内蔵されている。通常 SRAM として正常に動作するものの、微細化によりトランジスタのランダムばらつきが増加するため、規格範囲外の電圧条件では動作マージン不足によるビット不良が発生する。その不良アドレスがランダムに発生することに着目し、通常はメモリ機能を有する IP を必要に応じてチップ ID 生成機能として利用する方法を提案する。既存の SRAM IP 及び BIST 回路を使うことで面積オーバヘッドを最小限に留めることができる。また大規模 SRAM でランダムに発生する不良アドレスを用いることで高い一意性を得ることができるため、チップ ID の偽装・模倣に対する耐性向上が期待でき、SoC のセキュリティ向上面で有用性が高い。

③優位比較

これまで、ランダムばらつきを利用したチップ ID 生成方法は幾つか提案されているが、いずれも ID 生成専用ハード IP 化されたもので、面積オーバヘッドが大きく，ハードウェアの設計コストが発生する。本提案手法では、既存 SRAM 及び BIST を有効活用することで、面積オーバヘッドを最小限に抑えることができる。追加プロセスも必要とせず、小面積、低製造コストの面で他提案に比べて優位である。また、フューズのように固定長のチップ ID が存在する訳ではないため、タンパリング等による ID の盗難に対する耐性が高い。

(5)成果5.「マルチコアアーキテクチャの Virtualization 評価環境」

（吉本グループ+勝グループ＋於保グループ）

① 内容

自動車システムレベルにおけるディペンダブルメモリベースマルチプロセッサの機能安全性検証について、Virtualization を用いて実施するために、QoB メモリやレジスタの一括コピー機能/一括比較機能をモデル化した。本機能のモデルや、前年度まで開発した QoB メモリ故障注入機構に加えて、今年度は、新たにレジスタに故障が発生したときの Virtualization 評価を実現するために必要なレジスタ故障注入機構を実装し、メモリだけでなくレジスタ一括比較機能の評価が可能な Virtualization 環境を構築した。本 Virtualization 技術により、実機試作前に、ディペンダブルメモリアーキテクチャおよび回路技術の有効性を定量的に検証することが可能となる。

① 有用性

この検証手法を用いて、ディペンダブルメモリベース・マルチコアプロセッサによる自動車安全システムへの有効性検証を実施できる。また、種々の組込みシステムの信頼性検証手法として応用展開が期待できる。

② 優位比較

Virtualization によるシステムレベルでのマルチコアアーキテクチャのメモリ及びレジスタ故障時評価環境はこれまでになく画期的な成果である。

(6)成果6.「Dual コアアーキテクチャのエンジン制御応用デモ」

（吉本グループ+勝グループ＋於保グループ）

① 内容

これまで実施してきた Vrualization システム（Matlab/Simulink Simulator + Virtualizer Simulator）に加えて、車両モデルシミュレータとして、CarSim Simulator を結合することにより、SRAM のビット不良が実エンジン制御に及ぼす影響をシミュレーションにより定量的に導出するとともに、デモシステムとして構築した（図 5－1）。SRAM の電源電圧を変化させることで、システムエラーレートの変化を導出するシミュレーション手法を開発した（図 5－2）。

② 有用性

機能安全アプリケーションにおいて，リアルタイム性かつ高信頼なソフトウェア実行の可能なプロセッサが求められるが、車載システムの VLSI においてエンジンルームの厳しい環境や外部の雑音より電圧降下が発生するための対策の効果を定量的に評価できる手法として極めて有用である。また、このデモシステムは顧客開拓のための有用な武器となる。

③ 優位比較

SRAM への不良注入による最終システム（エンジン制御システムなど）での不良率を求める手法は世界初である。

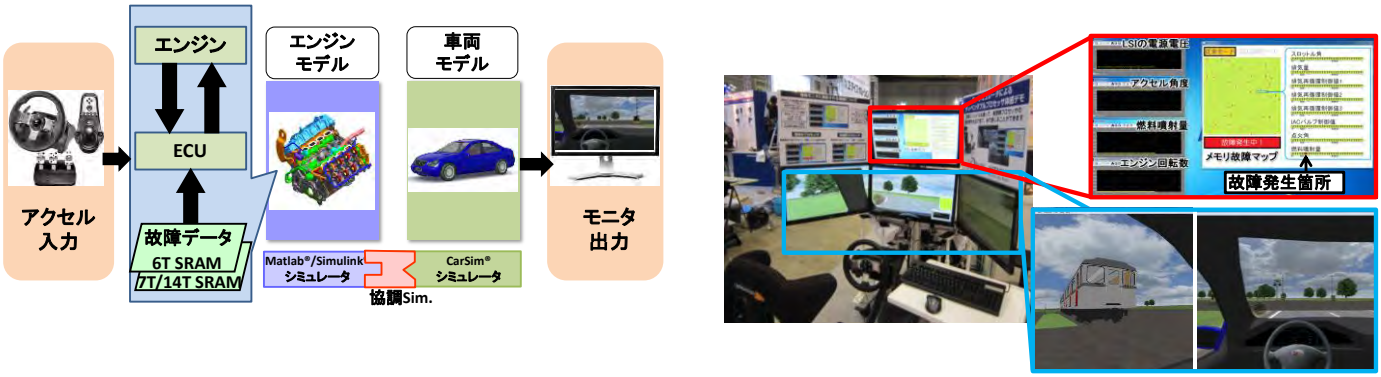


図 5－1　Dual コアアーキテクチャのエンジン制御応用デモシステム(ET2012 に於いてデモ展示)

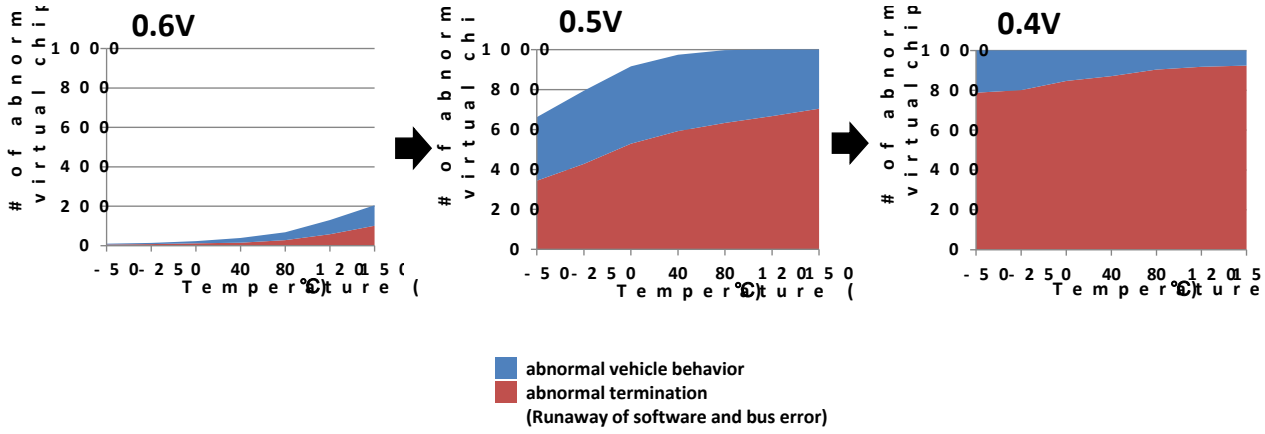


図 5－2　SRAM 不良に起因するエンジン制御動作の誤動作率の推移

3．2　上記3．1の成果うち、特筆すべきもの

(1)　特に顕著な成果(科学や技術の新しい分野の展望など)

○成果 1.「LSI チップ-パッケージ-ボード統合ノイズシミュレーションの高精度化」(永田グループ)

本研究成果により、電磁環境両立性(EMC)にかかる VLSI のディペンダビリティ設計において欠くことのできない、LSI チップにおける電源ノイズのシミュレーションを具体的に実現できる。研究初期より、主として小規模なデジタル回路を対象に、電源ノイズモデルの高精度化とモデル生成フローの確立について研究を進めてきたが、平成 24 年度の開発成果として、32 bit マイクロプロセッサを例題に、実用規模のデジタル回路における電源ノイズモデルを提供できることを示した。広い周波数範囲で電源ノイズ成分を予測できることから、動的な電源電流の変化が引き起こす EMC の解析に適している。近年の VLSI システム開発に一般化の進む「LSI チップ-パッケージ-ボード統合開発手法」において、とりわけ電源ノイズを考慮したディペンダブル設計に応用が期待できる。

○成果 4.「SRAM のランダムビット不良を利用したチップ ID 生成機構によるメモリベースセキュリティ技術の開発」(新居 G)

従来のチップ固有 ID 生成技術では、トランジスタのランダムばらつきに着目した種々の PUF ハードマクロが提案されているが、いずれも環境変動・ノイズ等に対する耐性が低く、温度・電圧変動に対して安定したIDを生成することが困難であるという課題があった。我々は、逆アシストにて発生したメモリ不良アドレスからIDを生成する方法を提案した。さらに製品出荷前のスクリーニングテストを用いた安定アドレスの抽出手法およびオンチップの不揮発素子を導入したメモリベースのチップID生成機構を開発、環境変動・ノイズ変動耐性が

高いことを実デバイスにて実証した。

○成果5.「マルチコアアーキテクチャの Virtualization 評価環境」(勝G、於保 G、代表者G)
車載システム非実機検証手法では、米国 GM 社、富士通テン社等が積極的に取り組んでいるが、マイコン模擬より抽象度の高いレベルで実行しているため精度が悪化しマイコン動作を模擬することができない。これに対し、本研究グループでは、今までに、マイコン模擬が可能な CPU モデルベースの協調シミュレーションが可能となるため、マイコン内にメモリ故障を注入でき、かつ注入したメモリ故障がシステムに与える影響を評価することができ、極めて精度の高いシステムレベルでのシミュレーション実行が可能となる。更に成果8により、マイコン内のメモリだけでなく、CPU 内のレジスタに関しても、故障注入ができる検証環境を構築することができるようになり、自動車業界でニーズが高い、マイコン内各場所での FMEA 解析ができる機能安全検証の実現が期待できる。

(2) 当初計画で想定外であった重要・新規な展開

§4. 成果発表等

(4－1)原著論文発表
●論文詳細情報

1. Takuya Sawada, Taku Toshikawa, Kumpei Yoshikawa, Hidehiro Takata, Koji Nii, Makoto Nagata, “Evaluation of SRAM-Core Susceptibility against Power Supply Voltage Variation,” IEICE Transactions on Electronics, Vol. E95-C, No. 4, pp. 586-593, DOI: 10.1587/transele.E95.C.586, Apr. 2012.
2. S. Yoshimoto, T. Amashita, S. Okumura, K. Nii, H. Kawaguchi, and M. Yoshimoto, "NMOS-Inside 6T SRAM Layout Reducing Neutron-Induced Multiple Cell Upsets," IEEE International Reliability Physics Symposium (IRPS), pp. 5B.5.1-5, Apr. 2012.
3. Yuta Sasaki, Kumpei Yoshikawa, Kouji Ichikawa, Makoto Nagata, “Co-Evaluation of Power Supply Noise of CMOS Microprocessor using On-Boar Magnetic Probing and On-Chip Waveform Capturing Techniques,” in Proc. IEEE 2012 International Meeting for Future of Electron Devices, Kansai (IMFEDK 2012), #S-1, pp. 70-71, May 2012.
4. J. Jung, Y. Nakata, S. Okumura, H. Kawaguchi, and M. Yoshimoto, "A Variation-Aware 0.57-V Set-Associative Cache with Mixed Associativity Using 7T/14T SRAM," IEEE Faible Tension Faible Consommation (FTFC), pp. 1-4, Jun. 2012.
5. S. Yoshimoto, T. Amashita, M. Yoshimura, Y. Matsunaga, H. Yasuura, S. Izumi, H. Kawaguchi, and M. Yoshimoto, "Neutron-Induced Soft Error Rate Estimation for SRAM Using PHITS," IEEE International On-Line Testing Symposium (IOLTS), pp. 173-176, Jun. 2012.
6. S. Yoshimoto, T. Amashita, S. Okumura, K. Nii, M. Yoshimoto, and H. Kawaguch, "Bit-Error and Soft-Error Resilient 7T/14T SRAM with 150-nm FD-SOI Process," IEICE Trans. Fundamentals, Vol. E95-A, No. 8, pp. 1359-1365, DOI: 10.1587/transfun.E95.A.1359, Aug. 2012.
7. Takuya Sawada, Hidehiro Takata, Koji Nii, Makoto Nagata, “Sensitivity of SRAM Operation against AC Power Supply Voltage Variation,” in Extended Abstracts of the 2012 International Conference on Solid State Devices and Materials (SSDM 2012), #J-3-1, pp. 1128-1129, Sep. 2012.
8. Hidehiro Fujiwara, Makoto Yabuuchi, Yasumasa Tsukamoto, Hirofumi Nakano, Hiroyuki Kawai and Koji Nii, “A Stable Chip-ID Generating Physical Uncloneable Function Using Random Address Errors in SRAM,” Proceedings of IEEE SoC Conference (SOCC), Sep. 2012.
9. S. Yoshimoto, T. Amashita, S. Okumura, H Kawaguchi, and M. Yoshimoto, "Multiple-Bit-Upset and Single-Bit-Upset Resilient 8T SRAM Bitcell Layout with Divided Wordline Structure," IEICE Trans. Electron., Vol. E95-C, No. 10, pp. 1675-1681, DOI: 10.1587/transele.E95.C.1675, Oct. 2012.
10. Takeshi Okumoto, Kumpei Yoshikawa, Makoto Nagata, “Monitoring Effective Supply Voltage within Power Rails of Integrated Circuits,” in Proc. 2012 IEEE Asian Solid-State Circuits Conference (A-SSCC 2012), #4-4, pp. 113-116, Nov. 2012.
11. Kumpei Yoshikawa and Makoto Nagata, “Co-simulation of AC Power Noise of CMOS Microprocessor using Capacitor Charging Modeling,” in Proc. IEEE CPMT Symposium Japan 2012 #19-2, pp. 293-296, Dec. 2012.
12. Kumpei Yoshikawa, Yuta Sasaki, Kouji Ichikawa, Yoshiyuki Saito, Makoto Nagata, “Co-simulation of On-Chip and On-Board AC Power Noise of CMOS Digital Circuits,” IEICE Transactions on Fundamentals, Vol. E95-A, No. 12, pp. 2284-2291, DOI: 10.1587/transfun.E95.A.2284, Dec. 2012.
13. S. Okumura, S. Yoshimoto, H. Kawaguchi, and M. Yoshimoto, “A 128-bit Chip Identification Generating

Scheme Exploiting Load Transistor's Variation in SRAM Bitcells,” IEICE Trans. Fundamentals, Vol.E95-A No. 12, pp.2226-2233, DOI:10.1587/transfun.E95.A.2226 , Dec. 2012
14. S. Okumura, S. Yoshimoto, H. Kawaguchi and M. Yoshimoto, "A Physical Unclonable Function Chip Exploiting Load Transistors’ Variation in SRAM Bitcells," IEEE Asia and South Pacific Design Automation Conference (ASP-DAC) University LSI Design Contest, pp.79-80, Jan. 2013.
15. Takuya Sawada, Hidehiro Takata, Koji Nii, Makoto Nagata, “False Operation of SRAM Cells under AC Power Supply Voltage Variation,” Japanese Journal of Applied Physics, (to appear)

(4－2)知財出願

① 平成24年度特許出願件数(国内 5 件)
② CREST 研究期間累積件数(国内 15 件)