様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１５　日現在

機関番号：　１２６０１
研究種目：　基盤研究(B)（一般）
研究期間：　2014～2017
課題番号：　２６２８００１２

研究課題名（和文）レジリエンス指向コンピュータシステムに関する研究

研究課題名（英文）Research on Resilience-Oriented Computer Systems

研究代表者
坂井　修一（Sakai, Shuichi）

東京大学・大学院情報理工学系研究科・教授

研究者番号：５０２９１２９０

交付決定額（研究期間全体）：（直接経費）　　13,200,000円

研究成果の概要（和文）：情報社会の飛躍的発展の中で、ITシステムの信頼性・安全性をこれまでより高い水準で確保することは喫緊の課題である。本研究では、ITシステムに故障や侵入があった場合でも、被害を最小限に食い止め、正常動作を続けさせるか、最小限のオーバヘッドで機能回復をする技術の研究開発を行った。具体的には、タイムボローによる遅延隠蔽、オンデマンドの細粒度部分再構成、ストリーム指向の防御、実時間的な異常予知などの新しい要素技術を提案・検証し、さらにこれらを統合して効率的に動作させるレジリエンス指向コンピュータを検討・提案し、テストベッドによってその有効性を示した。

研究成果の概要（英文）：Our information society is developing so rapidly that it is a pressing issue to keep the reliability and safety of IT systems at a much higher level than before. In this research, we have developed innovative technologies to minimize the damage and keep the correct operation or to restore functions with minimal overhead even if there is a breakdown or intrusion in the IT system. Specifically, we proposed and verified new element technologies such as delay concealment by time borrow, fine-grained partial reconstruction on demand, stream-oriented protection against attacks, real-time abnormality prediction, and integrated them to realize a resilience-oriented computer which efficiently operates all the functions. In addition, we have developed a testbed to prove its effectiveness.

研究分野：　情報システムとその応用

キーワード：　レジリエンス　信頼性　安全性　タイムボロー　ストリーム指向制御　異常予知　アーキテクチャ　可用性

１．研究開始当初の背景

第 4 期科学技術基本計画の中では、第 3 期に引き続いて「安全、かつ豊かで質の高い国民生活を実現する国」が最重要の基本理念の１つとして据えられている。この理念を実現するためには、情報インフラが「安全・安心」であることが必須であり、このことは、日本だけでなく地球規模で日々その重要性を増している。

情報技術の最も基本にあるのが情報処理技術と通信網の技術であり、端的にそれはコンピュータとインターネットの技術である。すなわち、「安全・安心なコンピュータとインターネットを構築すること」が、今の情報技術に最大の課題といってよい。ここでは、このうち前者の「安全・安心なコンピュータ」の構築をめざし、アーキテクチャ技術とソフトウェア技術を中心に研究する。

「安全・安心」は、信頼性・安全性・可用性・堅牢性などの複合したものである。過去においても、コンピュータのこれらの機能を向上させることは重要なテーマであり、多重化技術、暗号技術、耐タンパ技術などによってその向上が図られてきたが、(1)ソフトウェアの複雑化とブラックボックス化、(2)ゲート規模の爆発的増加による LSI の複雑化、(3)ネット社会の急激な進展による攻撃の多様化と社会的影響の増大、(4)通信やソフトウェアの信頼性におけるベストエフォート文化の浸透、の 4 点によって、近年になってさらに問題が複雑化・大規模化・多様化している。

このような現状を受けて、国内外の多くの研究機関で、コンピュータの信頼性や安全性をアーキテクチャ技術・ソフトウェア技術によって向上させる試みがなされている。代表例を示せば、(1)タイミング故障耐性を向上させるミシガン大学の Razor や九州大学の Canary、(2)タンパ耐性をもつアーキテクチャとしてスタンフォード大学の XoM、MIT の AEGIS、東芝 L-MSP、(3)アタック耐性をもつアーキテクチャとして MIT の DIFT、プリンストン大学の RIFLE、九州大学の実行監視方式、(4)インジェクションアタックを防ぐ方式としてのスタンフォード大学の Raksha などがこれである。これらは、プログラムレベルやスレッドレベル、命令レベル、アーキテクチャレベルにおいて信頼性・安全性を向上させる優れた要素技術を提案しているが、故障や侵入を完全に防ぐことができるわけではなく、万が一に故障や侵入があった場合、被害を最小限に食い止めたり、最小限のオーバヘッドで機能回復したりすることが十分に考えられているわけではない。

研究代表者は、コンピュータのアーキテクチャおよびソフトウェアを中心課題として、30 年以上に渡って研究を行ってきた。1980 年代から今日まで、研究代表者は、マイクロプロセッサの効率化・省電力化の研究を行い、データフロー方式の改良、大規模データパスプロセッサの提案・評価、スーパスカラ方式の究極的高性能化、省電力チップマルチプロセッサのアーキテクチャおよび最適化コンパイラの提案などの研究開発を行った。提案したマイクロプロセッサは、実際に EMC-R、RICA-1 など VLSI チップ上に実装され、あるいは詳細レベルのシミュレーション評価によって高い効率が検証された。成果は国内外で高い評価を得ており、IEEE Outstanding Paper Award、日本 IBM 科学賞など、多数の賞を受賞している。

以上の研究を通じて高性能で低消費電力のコンピュータの研究開発を行い、高性能・省電力コンピュータアーキテクチャの確立という点で大きな成果をあげたが、一方で性能、消費電力、信頼性・安全性の３者はトレードオフの関係になることが多く、性能と消費電力の２つだけを扱うことの限界を認識せざるをえなかった。結果として、コンピュータにおける信頼性・安全性の研究の必要が痛感されたのであった。

2000 年代に入り、以上の成果をふまえ、また上記(1)(2)(3)(4)で述べた問題認識のもとに、性能・省電力と並ぶ第三の軸として、信頼性・安全性について特に深く研究することとなった。具体的には、JST CREST プロジェクト「ディペンダブル情報処理基盤」（申請者が代表）において、プロセッサアーキテクチャ、OS、応用ソフトウェアまでのセキュリティおよび信頼性の基本技術を研究開発した。本プロジェクトによって、近未来の IT に必要な高信頼化・高い安全化技術が新規に提案され一部検証された。この成果を受けて、JST CREST プロジェクト「アーキテクチャと形式的検証の協調による超ディペンダブル VLSI」（申請者が代表）において、高信頼化の研究を進める(2007 年 10 月～2012 年 9 月)とともに、STARC 共同研究「超ディペンダブルプロセッサの研究」(2007 年 4 月～2010 年 3 月)、科研基盤（B）「超セキュアプロセッサに関する研究」(2010 年 4 月～2013 年 3 月)において、マイクロプロセッサのセキュリティを飛躍的に向上させる研究を行った。これらにおいて、タイミング故障、永久故障、インジェクション攻撃などに高い耐性をもつコンピュータの新規提案・評価検証を行い、国内外での論文発表や国際特許などの成果をあげた。一方で、故障や攻撃への「完全な防御」は不可能であり、従来の防御や緩和技術に加えて、故障や侵入があった場合でも、被害を最小限に食い止め、正常動作を続けさせるか、最小限のオーバヘッドで機能回復する技術の研究開発が重要であることを痛感した。

２．研究の目的

本研究では、IT システムに故障や侵入があった場合でも、被害を最小限に食い止め、正常動作を続けさせるか、最小限のオーバヘッドで機能回復する技術の研究開発を行う。従来、故障対策は多重化によるものが、攻撃

対策はパターンマッチによる侵入検知と暗号化によるものが主流であった。本研究では、予測・検知が困難でこれまでは防ぐことが困難であった故障や攻撃に耐性のあるコンピュータシステムの構築をめざす。そのために、タイムボロー、オンデマンドの細粒度部分再構成、ストリーム指向の防御、異常予知などの新しい要素技術を提案する。さらに、これらを統合して効率的に動作させるレジリエンス指向コンピュータを検討・提案し、テストベッドを試作して動作を実証する。

特にここでは、対象を現在最も重要と思われる(1)タイミング故障、(2)永久故障、(3)インジェクション攻撃、(4)ゼロデー攻撃 の４つに絞って、コンピュータのレジリエンス（耐久力・復元力）を飛躍的に高める技術を研究開発する。特に、防止・防御がむずかしい故障・攻撃に対して、効率的に縮退運転をする技術や最小限のオーバヘッドで機能回復をする技術の研究開発を行う。具体的には、新規要素技術を提案し、プロセッサ・シミュレータや FPGA 上での実装、ソフトウェア開発を行って機能を検証し、あわせて動作性能および消費電力についても評価する。その上で、提案した技術を統合的に扱うための制御機構を提案し、シミュレーションおよび FPGA などによる実装、ソフトウェアの動作試験などによって機能を検証する。さらに、４種類のレジリエンスをもつプロセッサのテストベッド実装と動作検証、性能と消費電力の全体シミュレーション評価までを行う。

３．研究の方法

レジリエンス要素技術として、タイムボローによる遅延隠蔽、オンデマンドの細粒度部分再構成、ストリーム指向の防御、実時間的な異常予知のそれぞれの研究を行い、成果を提案者が開発した詳細シミュレータ「鬼斬Ⅱ」に新規機能を組み込む、ソフトウェアを開発するなどして評価し、さらにプロトタイプ実装などによって実証的に検証する。さらに、これらを統合管理するレジリエンス・マネジャの機能・機構を明らかにし、レジリエンス指向コンピュータの全体を設計する。コンピュータの中心となるプロセッサについては、「鬼斬Ⅱ」を改良する形で詳細シミュレータを作成し、FPGA テストベッドによる実装を行い、さらに必要に応じて VDEC などを使ったカスタム VLSI 実装を行う。最後に、スタンドアロンな情報システムとしてのレジリエンス指向コンピュータの動作検証、達成される信頼性・安全性の検証、実行効率測定、消費電力測定などを行い、本研究成果の有効性を検証する。

４．研究成果

4.1 タイミング・フォールトの緩和

VLSI のワーストケース設計では、素子遅延のばらつきによって、回路本来の実行速度が得られなくなっている（図 1）。研究代表者らは、ワーストケースではなく、実際の回路遅延に基づいた動作の実現を目的として、新しいクロッキング方式を提案、これを検証してきた。

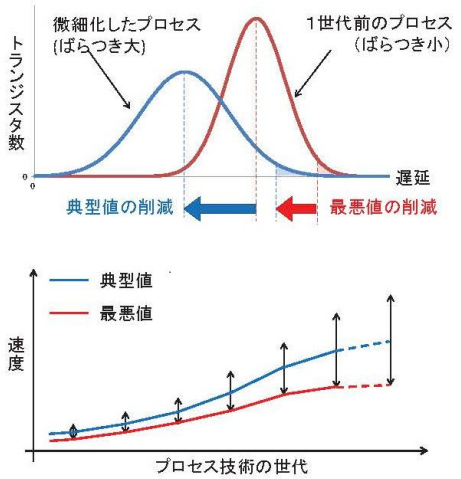

図 1. VLSI の世代と遅延の典型値・最悪値

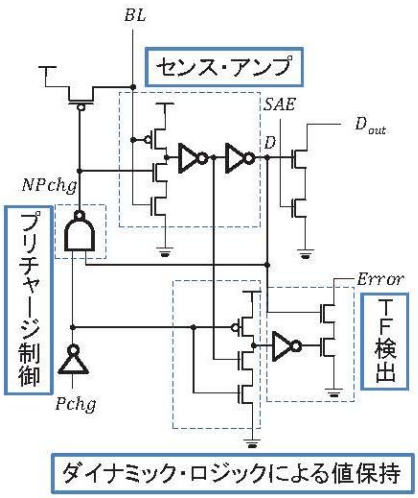

図 2. 提案手法の回路実装

本科研費の研究では、以下のことを行った。

(1) ダイナミック・ロジックへの動的タイミング・フォールト検出手法の適用

ダイナミック・ロジックでは、プリチャージ動作がタイミング・フォールトをマスクするため、従来のフォールト検出手法は適用できない。そこで、ダイナミック・ロジックの評価結果に応じて、プリチャージの有無を制御することによって、検出手法の適用を可能にする提案を行った（図 2）。そして、本提案を適用したレジスタファイルをトランジスタ・レベルで設計し、SPICE シミュレータ上でタイミング・フォールトを検出できることを確認した。

(2) 動的タイム・ボローイングを可能にする

クロッキング方式のための二相ラッチ生成アルゴリズム

研究代表者らの提案するクロッキング方式を、具体的なディジタル回路に適用する手法について、二相ラッチ化のアルゴリズムを提案した。

二相ラッチ化の要件は、全てのパスに逆相ラッチがそれぞれ1つだけ挿入されていることである。二相ラッチ化の目標は、挿入する逆相ラッチの数を少なくすることと、パスの遅延ができるだけ二分されるようにすることである。二相ラッチ化のアルゴリズムとして、全てのパスに逆相ラッチが挿入されるまでパスをイテレートして挿入対象ネットを探索することで二相ラッチ化の要件を満足させる。また、各逆相ラッチを挿入するのにコストが必要だとみなして、コストの総和が最小となるものを探索することで、目標達成をはかる。

本アルゴリズムを、規模の異なるキャリルックアヘッドに適用した結果、効率良く二相ラッチ化回路が生成されることが示された。

本アルゴリズムは、回路素子の静的解析を用いるなどの改良によって、さらに良い回路を効率的に生成することが可能になった。さらに、積和回路に改良アルゴリズムを適用し、効果を確認した。

アルゴリズムのさらなる改良、より複雑な回路への適用などが今後の課題となっている。

4.2 ストリーム指向の攻撃検知・防御

IT システムへの様々な攻撃を検知・防御するための機構として、文字列操作単位でテイント伝播を追跡する手法である SWIFT を考案している（図 3）。本科研費の研究では、SWIFT について以下のことを行った。

(1) SWIFT によるゼロデイアタック検出

SWIFT の実現例である PHP-SWIFT について、ゼロデーアタックなどの未知の攻撃に対して適応できるかどうかの評価を行った。最初に、WordPress 上に SQL インジェクションに対する脆弱性のある環境を再現し、攻撃を仕掛けることで評価を行った。その結果、SWIFT の機構は有効に機能し、多くの場合でゼロデイアタックの検出に成功した。一方で、SWIFT でも防ぐことができなかった攻撃も発見され、伝播規則や実装についてさらに検討が必要であることがわかり、改良を進めている。また、ディレクトリ・トラバーサルやクロスサイト・スクリプティングに対しても耐性をもつかどうか、現在研究中である。

(3) Android におけるプロセスベースのテイント伝播を用いた個人情報漏洩検知システム

近年、スマートフォンにおける個人情報漏洩の被害が急増しているため、これを防ぐ対策が喫緊の課題となっている。ここでは、プロセスベースのテイント伝播情報を SELinux に組み込むことにより、ユーザ空間の脆弱性にかかわらず、オーバヘッドをほとんど生じない OS レベルでの個人情報流出検知システムを提案し、評価を行った。その結果、個人情報の流出をきちんと検知できること、オーバヘッドもほぼ生じないことが確認された。

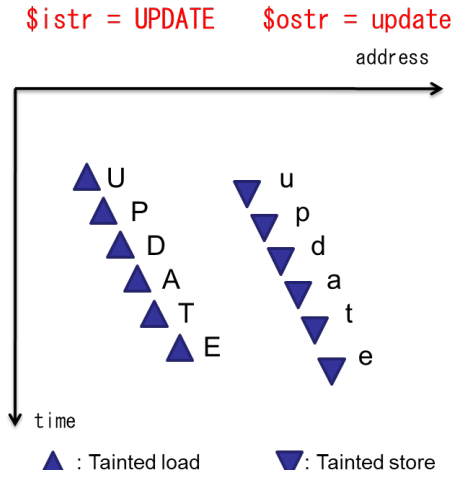

図 3. SWIFT の原理図

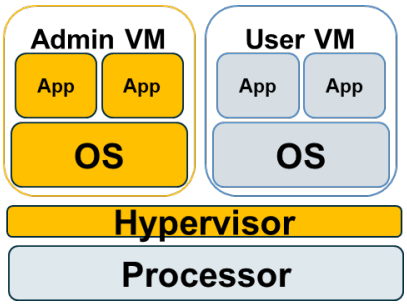

図 4　VM セキュアプロセッサ概念図

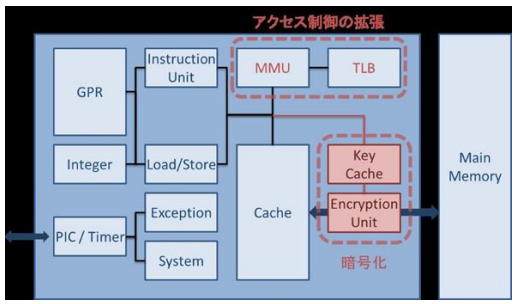

図 5　Sharkcage の構成

4.3 セキュアプロセッサ

セキュリティ機能をアーキテクチャレベルでもつプロセッサをセキュアプロセッサと呼ぶ。これに関して本科研費を用いて、以下の研究を行った。

(1) ユーザ VM を守るプロセッサアーキテクチャの研究

クラウド環境で悪意の第三者からユーザデータを守る VM セキュアプロセッサ Sharkcage を考案し（図 4)、そのアーキテクチャを提案（図 5)、設計によってその有効性を検証した。Sharkcage では、ユーザ VM 全体が保護されるため、外部からはもとより、管理 VM などシステムの内側からの攻撃に対してもユーザデータが守られる。

(2) クラウドフォレンジックに向けた VM セキュアプロセッサ

クラウドコンピューティングの普及に伴いクラウドフォレンジックの需要も増しているが、クラウドフォレンジックは通常のフォレンジックと比べて効率面やセキュリティ面で課題が多い。研究代表者らは、そのようなクラウドフォレンジックの課題を解決するために、ハードウェアによるログファイル管理に注目した。特にログファイルの機密性。完全性・真正性を確保するために、暗号化やハッシュ値・電子署名生成機能を組み込んだ VM セキュアプロセッサの開発を進めている。本科研費の研究では、クラウドフォレンジックの課題を解決するために VM セキュアプロセッサを導入したログファイル管理システムの提案を行い、それに必要な VM セキュアプロセッサの設計と実装を進めた。評価の結果、従来のソフトウェアベースのフォレンジック手法よりも強固かつ効率的であることが示された。

(3) セキュアプロセッサにおける楕円曲線暗号の評価と実時間的な異常検知

セキュアプロセッサではユーザプロセスの認証のために電子署名を使うが、そのさいに公開鍵暗号が使われる。これまで、公開鍵暗号として RSA 暗号が使われてきたが、本研究では、楕円曲線暗号を用い、さらに回路をハードウェア化することで軽量高速な認証が可能となることを、設計・実装による評価によって示した。

本研究によって、実時間的な異常検知についても実現性に向けての一歩を進めることができた。

(4) セキュアプロセッサを用いたマルチプロセッサシステムの設計

セキュアプロセッサは暗号化機構と完全性検証機構によってデータを保護するが、現状ではその普及が進んでいるとは言えない。この理由の１つに、セキュアプロセッサがマルチプロセッサ環境に対応していないことのよるパフォーマンスの低下が挙がられる。本科研費による研究では、セキュアプロセッサを用いてマルチプロセッサシステムを構築することでパフォーマンスの向上を目指し、その設計を行った。その結果、本システムは現実的なコストで実装でき、十分なパフォーマンスが得られることが検証された。

(5) セキュアプロセッサ利用環境における DMA の実現手法

セキュアプロセッサの利用環境下では、信頼性担保のため、従来の外部デバイスによる DMA(Digital Memory Access)を適用することができない。本研究では、信頼できる外部デバイスの存在を仮定し、本来の DMA に期待されるプロセッサからの負荷のオフロードとデータの秘匿性・完全性を両立した DMA を実現するためのモデルを提案し、設計・評価して脆弱性のない DMA が実現されることを検証した。

4. 5　全体統合

全体統合のベースとして、従来のスーパスカラ・アーキテクチャを軽量・高速化した新しいアーキテクチャを提案、シミュレーションと FPGA 実装によって、電力性能比などにおける有効性を検証した。

さらにこのベース・プロセッサにセキュリティ機構を導入し、VM セキュアプロセッサ Sharkcage を設計した。

タイムボロー方式によるクロッキングは、実際にこれをカスタムチップとして設計するときに用いることができる。

ストリーム指向のテイント追跡技術を組み込んだ PHP-SWIFT は汎用ソフトウェアであり、PHP 処理系のあるプロセッサであれば、これを動作させられる。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

① 坂井 修一: 情報社会と人間，サイバースペースとセキュリティー 第 5 回，情報管理：Vol. 59 No. 11 p. 768-771 (2017).

② Junji YAMADA, Ushio JIMBO, Ryota SHIOYA, Masahiro GOSHIMA, and Shuichi SAKAI: Skewed Multistaged Multibanked Register File for Area and Energy Efficiency, IEICE TRANS. INF. & SYST., VOL.E100-D, NO.4 pp.822-837, (2017)

③ MinSeong Choi, Masahiro Goshima and Shuichi Sakai: An Inductive Method to Select Simulation Points, IEICE Transactions on Inforamtion and Systems, E99-D(12), pp. 2891-2990 (2016)

④ Naruki KURATA, Ryota SHIOYA, Masahiro GOSHIMA, Shuichi SAKAI: Address Order Violation Detection with Parallel Counting Bloom Filters,IEICE Transactions on Electronics Vol. E98.C, No. 7, pp. 580-593 (2015).

〔学会発表〕（計 18 件）

① 甲地 弘幸, 入江 英嗣, 坂井 修一：プリ

フェッチラインの再参照間隔を予測するキャッシュマネジメント 情報処理学会研究報告 2017-ARC-227, No. 12, pp. 1–8 (2017)
② 谷合 廣紀, 宮永 瑞紀, 入江 英嗣, 坂井 修一: セキュアプロセッサにおける楕円曲線暗号の評価, 情報科学技術フォーラム講演論文集, No. 4, CL-004 (2017).
③ 入江 英嗣:コンピュータを作る, 使う, 情報科学技術フォーラムイベント企画「東大・情報理工研究 100 連発 ～電子情報学専攻編～」 (2017).
④ 坂井 修一、入江 英嗣:未来のコンピュータ, 未来のコンピューティング, 情報科学技術フォーラム展示会 (2017).
⑤ 島田 伸夫, 谷合 廣紀, 宮永 瑞紀, 入江 英嗣, 坂井 修一: 侵入検出手法 SWIFT によるゼロデイアタック検出, 信学技報, vol. 116, no. 510, CPSY2016-149, pp. 321-326 (2017).
⑥ 鈴木 璃人, 梶原 拓也, 宮永 瑞紀, 入江 英嗣, 坂井 修一: セキュアプロセッサ利用環境における DMA の実現手法, 信学技報, vol. 116, no. 510, CPSY2016-138, pp. 39-44, (2017).
⑦ Mizuki Miyanaga, Hidetsugu Irie, Shuichi Sakai: Accelerating Integrity Verification on Secure Processors by Promissory Hash, 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 22-29 (2017)
⑧ 梶原 拓哉, 宮永 瑞紀, 入江 英嗣, 坂井 修一: セキュアプロセッサを用いたマルチプロセッサシステムの設計, 電子情報通信学会技術研究報告, Vol.116, No. 240, pp. 7–10 (2016)
⑨ 西川 卓, 塩谷 亮太, 入江 英嗣, 五島 正裕, 坂井 修一: フィルタを用いたメモリ・アクセス順序違反検出手法の評価, 情報処理学会研究報告, Vol. 2016-ARC-219, No. 15, pp. 1-6 (2016)
⑩ 津坂 章仁, 谷川 祐一, 広畑 壮一郎, 五島 正裕, 入江 英嗣, 坂井 修一: 動的タイム・ボローイングのための二相化アルゴリズムの改良と評価, 電子情報通信学会技術研究報告, Vol. 115, No. 518, pp. 133-138 (2016).
⑪ 千田 拓矢, 谷合 廣紀, 宮永 瑞紀, 入江 英嗣, 坂井 修一: クラウド フォレンジックに向けた VM セキュアプロセッサの設計と実装, 電子情報通信学 会技術研究報告, Vol. 115, No. 518, CPSY2015-143, pp. 115-120 (2016).
⑫ 今田 丈雅, 宮永 瑞紀, 入江 英嗣, 坂井 修一: Android におけるプロセスベースのテイント伝搬を用いた個人情報の漏洩を検知するシステム, 電子情報通信学会総合大会, A-7-3, pp.89 (2016)
⑬ 西川 卓, 塩谷 亮太, 入江 英嗣, 五島 正裕, 坂井 修一: Bloom-like SVW の評価,電子情報通信学会技術研究報告, Vol. 115, No. 243, pp. 27–34 (2015).
⑭ 西川 卓, 塩谷 亮太, 入江 英嗣, 五島 正裕, 坂井 修一: メモリ・アクセス順序違反検出手法の評価, 電子情報通信学会技術研究報告 信学技報 , No. 115(174), pp. 21–29 (2015).
⑮ 神保 潮, 五島 正裕, 坂井 修一: タイミング・フォールト検出手法の RAM への適用,情報処理学会研究報告 2015-ARC-214 , No. 8, pp. 1–8 (2015).
⑯ 酒井 一憲, 津坂 章仁, 神保 潮, 五島 正裕, 坂井 修一: 回路素子の静的解析を用いた二相化アルゴリズムの改良,情報処理学会第 77 回全国大会論文集 , No. 1, pp. 77–78 (2015).
⑰ 津坂 章仁, 谷川 祐一, 広畑 壮一郎, 五島 正裕, 坂井 修一: 動的タイム・ボローイングを可能にするクロッキング方式のための二相ラッチ生成アルゴリズム, 情報処理学会研究報告 2014-ARC-211 , No. 9, pp. 1–10 (2014).
⑱ 神保 潮, 山田 淳二, 五島 正裕, 坂井 修一:ダイナミック・ロジックへのタイミング・フォールト検出手法の適用、情報処理学会研究報告 2014-ARC-210 , No. 18, pp. 1–8 (2014).

〔その他〕
ホームページ
http://www.mtl.t.u-tokyo.ac.jp/

６．研究組織

(1)研究代表者
坂井　修一　（Sakai Shuichi）
東京大学・大学院情報理工学系研究科・教授
研究者番号：　50291290

(2)研究分担者
五島　正裕　（Goshima Masahiro）
東京大学・大学院情報理工学系研究科・准教授（当時）
研究者番号：　90283639

入江 英嗣　（Irie Hidetsugu）
東京大学・大学院情報理工学系研究科・准教授
研究者番号：　50422407