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

令和　５ 年　 ５ 月 ３０ 日現在

機関番号：１６３０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１８７８

研究課題名（和文）つながるデバイスのフィールドテストのための信頼性強化設計法の開発

研究課題名（英文）Study of Design for Trust for Field Test of Connected Devices

研究代表者
高橋　寛（Takahashi, Hiroshi）

愛媛大学・理工学研究科（工学系）・教授

研究者番号：８０２２６８７８

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：Society 5.0を実現するためには，つながることを前提としたデバイス（集積回路）の高信頼化が必要である。集積回路の信頼性を低下させる要因は，「故障」および「侵害」である。この研究計画では，市場稼働時に，フィールドテストとして組込みテストで集積回路自身によって故障を検出する手法および安全にフィールドテストを実行する手法を信頼性強化設計（Design for Trust）として提案する。

研究成果の学術的意義や社会的意義
本研究の成果は，つながることを前提としたデバイス（集積回路）の高信頼化において意義がある。具体的には，つながるデバイスの市場稼働時において高信頼性を保証するために，フェイールドテストやセキュアーなテスト環境の構築ができる信頼性強化設計法を提案したことである。この研究の社会的が意義は，つながるデバイスの信頼性を向上するための基盤技術を確立できたことである。また研究成果の学術的な意義は，車載システムのフィールドテストの実現およびエッジデバイスのセキュリティ強化の実現など競争的な研究領域においても，研究の新規性・有効性が評価され，当該分野で権威のある論文誌などに採択されたことである。

研究成果の概要（英文）：In order to realize Society 5.0, the devices (the integrated circuits) must be made highly reliable, based on the premise that they are connected. Faults and infringements reduce the reliability of the integrated circuits. In this study, we propose a non-destructive method to detect faults by the built-in self-test as a field test and a method to execute the field test safely as “Design for Trust”.

研究分野：計算機システム

キーワード：フィールドテスト　つながるデバイス　信頼性強化設計法

1. 研究開始当初の背景

情報社会基盤を構成するコンピュータの構成要素であるデバイス（集積回路）の高信頼化は，情報社会基盤の高信頼化のために必要である。Society 5.0 のためには，つながることが前提となるデバイス（集積回路）が正常でなければ，その集積回路を介してクラウドに不正確なデータが収集されてしまい，その結果としてクラウドで実施するデータ解析に基づく判断を誤ったものにする恐れがある。これまでに集積回路の高信頼化のためには，出荷時の製造テストの高精度化・高効率化法の提案や運用時の障害を回避するためのユーザ回路の冗長・多重化手法が提案されてきた。しかしながら，稼働時のフィールドテストではテスト実行時のさまざまな制約のもとでのテスト技術開発となるため，その技術は未だに確立していない。そこで，以下の課題がある。

課題1：市場で稼働時のフィールドテストでは，「テスト実行時間」，「故障検出率」，「消費電力」，および「テスト容易化設計の面積オーバヘッド」のそれぞれがトレードオフ関係にあるため，フィールドテストのためのテスト容易化設計法を確立しなければならない。

課題2：メモリコンピューティングデバイスのフィールドテストを確立しなければならない。

課題3：つながるデバイスの信頼性向上のためには，集積回路の真贋判定やフィールドテスト時のセキュリティ確保などを安全なフィールドテスト環境で実施しなければならない。

2. 研究の目的

①集積回路に対するフィールドテストのために故障検出強化技術を開発する。

②メモリコンピューティングデバイスにおける故障状態警告技術を開発する。

③つながるデバイスにおいて，テスト容易化技術を利用して集積回路のフィールドテストをセキュアーなテスト環境で実行する技術を開発する。

3. 研究の方法

本研究では以下のサブテーマにおいて研究を進めた。

サブテーマ① 集積回路に対するフィールドテストおいて，より少ないテストパターンの利用でも高い故障検出率を得ることができる故障検出強化技術を提案する。提案する故障検出強化技術は 2 つの機能を備える。論理回路の多時刻展開回路によってテストするマルチサイクルテストにおいて，「中間観測のための可観測性向上機能」および「強制的に論理値を反転させる可制御性向上機能」をフィールドテストのためのテスト容易化設計法として提案し，その挿入箇所の選択法を提案した。

サブテーマ② IoT 環境でのエッジコンピューティングデバイスとして新規に開発されているメモリコンピューティングデバイスのフィールドテストを実現するために故障状態警告技術を提案する。新規開発デバイスのメモリコンピューティングデバイスは，メモリセルであるルックアップテーブル(LUT)で構成される。新規メモリコンピューティングデバイスにおいては信頼性向上化のためのテスト容易化設計法は未だ議論されていない。そこで，本研究計画では，デバイスがフィールドで稼働時の論理回路の状況をメモリセルのチェーン構造で保存し，それを用いて動作状態を評価する故障状態警告技術を提案する。

サブテーマ③ つながるデバイスにおいて，テスト容易化技術を安全に利用して集積回路をフィールドテストする技術を開発する。テスト容易化設計法としてバンダリスキャンシステム（JTAG）を活用して，つながるデバイスに対して，非破壊で集積回路を安全にテストするためにセキュアーな JTAG システムのテストアクセス機構を提案する。

4. 研究成果

サブテーマ①に対する成果：フィールドテストおいて，より少ないテストパターンでテストを実行するためにマルチサイクルテストが提案されている。本研究では，課題の定式化として，マルチサイクルテストではマルチサイクルにおける多時刻展開回路を扱うため「故障影響の消失問題」および「故障検出能力の低下問題」が顕在化することを明らかにした。次に，その課題を解決するために，テストの最中に，フ

リップフロップの値を獲得できる中間観測のための可観測性向上機能として故障検出強化フリップフロップを提案した。次に，マルチサイクルテストにおいて，時刻が進む過程で，フリップフロップの値が固定化することを避けるために，強制的に論理値を反転させる可制御性向上機能として自己反転回路を提案した。図1に故障検出強化フリップフロップの概要を示し，図 2 に自己反転回路の概要をそれぞれ示す。

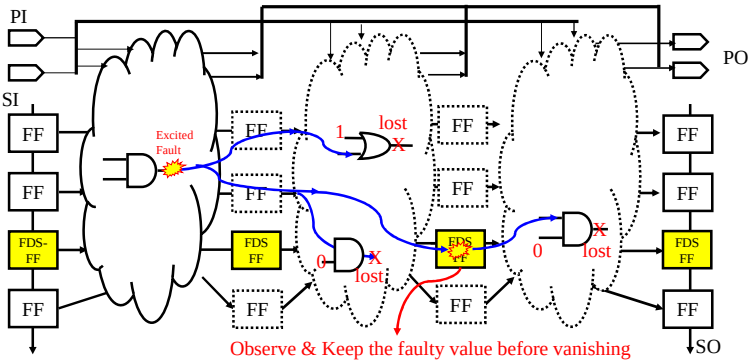

図1　故障検出強化フリップフロップの概要

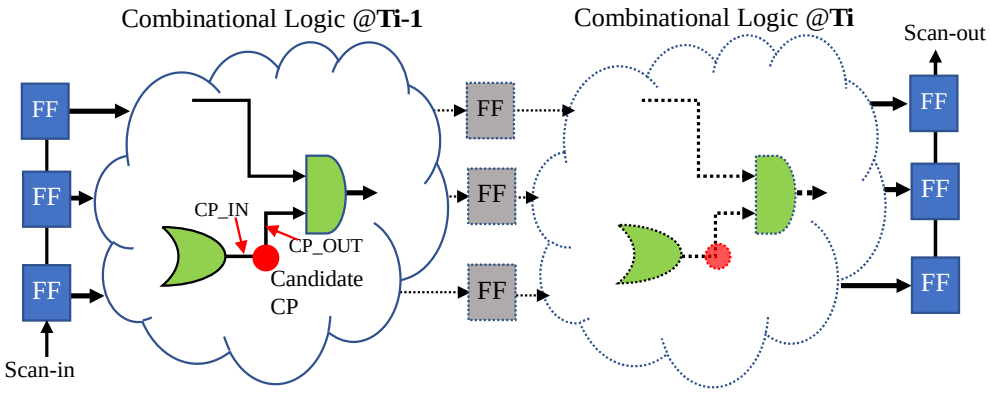

図2　自己反転回路の概要の概要

次に，できるだけ少数のテストパターンによって，設定した故障検出率を得るために効果的な故障検出強化フリップフロップと自己反転回路の挿入箇所の選択法を提案した。

提案法では，まず，すべてのフリップフロップが中間観測可能であると仮定して，マルチサイクルテストに拡張した評価値に基づいて自己反転回路の挿入箇所を選択する。次に，自己反転回路が挿入された多時刻展開された回路に対して，回路の構造的な情報に基づく評価値を利用して，予め設定された数のフリップフロップを検出強化フリップフロップとして選択する。

提案手法の有効性を評価するために，提案法を ISCAS89 ベンチマーク回路および ITC99 ベンチマーク回路に適用した評価実験結果を図 3 に示す。

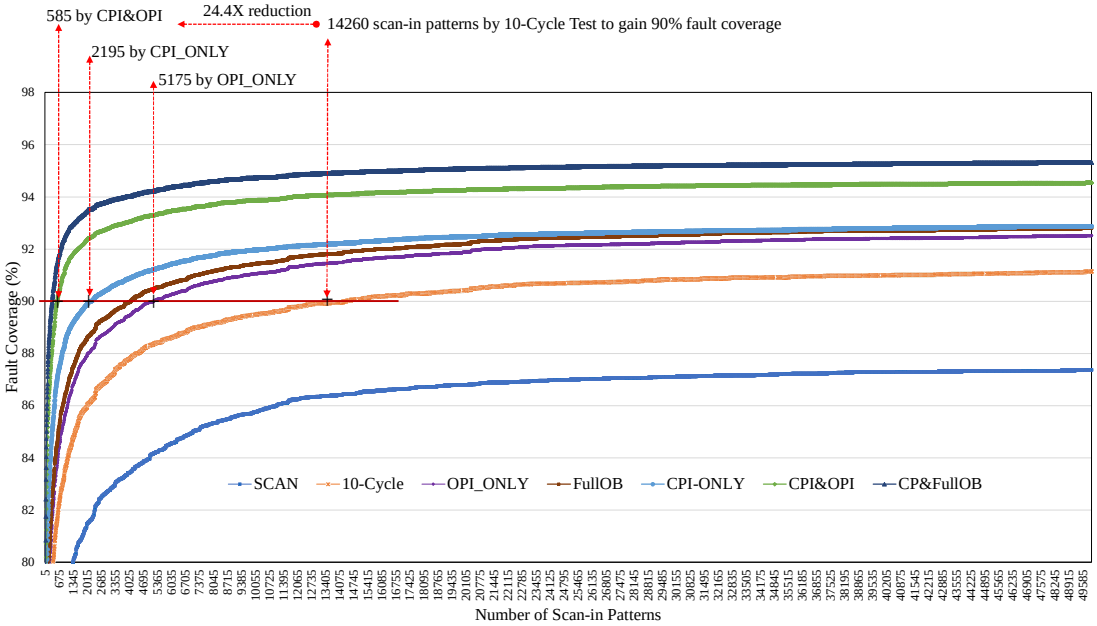

図3　提案法と従来法の比較

評価実験結果から，単一縮退故障検出率 90%を得るために，従来の 10 サイクルテストでは，14,260 パターンが必要であったが，回路の信号線の 1%に自己反転回路を挿入し，20%のフリップフロップを故障検出強化フリップフロップに置換した回路においては，585 パターンで単一縮退故障検出率 90%を得ることができた。

サブテーマ②に対する成果：フィールドテストにおける回路の内部状態の獲得技術に関して，文献調査を行った。「故障状態警告技術」としては，リングオシレーターを書き換え可能デバイス上に実装した。

MRLD は複数の汎用メモリセル（MLUT: Multiple Look Up Tables）をアレイ状に並んで構成されている。従来の再構成論理デバイス FPGA と比較して，MRLD では配線論理も直接 MLUT に構成するため，小遅延・低消費電力の優位性がある。

MRLD のグローバル遅延を測定するには，図 4 に示すように，MLUT アレイの個々の MLUT に RO の発振素子インバータを配置することが必要である．RO の発振動作時に，個々MLUT に構成されたインバータ論理による信号遷移が発生する。MLUT ではメモリに書き込まれたデータ（真理値表）を読み出す動作（アドレス入力，データ出力）のため，メモリでの劣化による遅延が起こると信号遷移時間が遅れてしまい，RO の出力で一定時間の発振周波数を観測することで MLUT 全体のグローバル遅延時間を計算することが可能である。計測したグローバル遅延時間を RO が通過した MLUT の数との平均値を取ると，MLUT 単体の平均遅延を得ることができる。

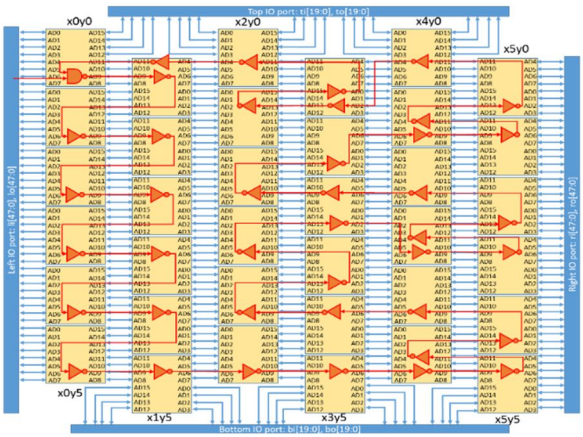

図 4 RO による MRLD のグローバル遅延測定

サブテーマ③に対する成果： 標準的なテストアクセス機構 (JTAG) にセキュリティ対策を講じないと、悪意のある攻撃者が JTAG を介してデバイスを乗っ取り、インターネットを介して IoT システムに対する攻撃を行うことができることがわかった。そこで，JTAG において，権限を持つユーザーのみに対してテストアクセスポートへアクセスを許可するアクセス制御方法として軽量な認証法である SAS-L というワンタイムパスワード認証方式に着目し，軽量な JTAG 認証プロトコルを提案した。

図 5 は，SAS-L2 を用いて JTAG アクセス認証プロトタイプを示す。JTAG における SAS-L2 認証方式の実現には，製品の出荷前にメーカによるデバイスとユーザの識別情報(デバイス ID とパスワードなどの情報)を暗号化し，初期登録情報としてデバイスのメモリに書き込むことが必要である製品ごとのデバイス識別情報とユーザ情報を管理するために，メーカ側はデバイス管理サーバ(DMS)を用意することが必要である。製品の出荷後，ユーザはデバックツールを用いて，DMS サーバと JTAG デバイスの間で認証手続きを行う。

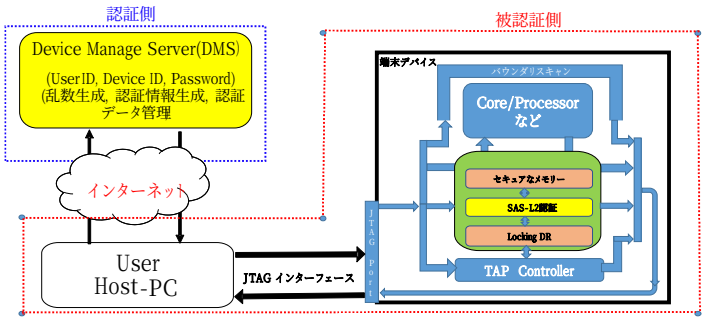

図 5 SAS-L2 による JTAG 認証プロトタイプ

評価実験として，設計した SAS-L2 を用いた JTAG 認証回路に対して ModelSim によってシミュレーションを実行し，認証が成功し，JTAG のロックが解除されていることが確認できた。提案法と従来法を書き換え可能なデバイス FPGA に実装した際のロジックセルの数および JTAG 攻撃対策効果を明らかにした。回路規模について比較を行った結果，ロジックセルの数が提案法は AES 暗号化機能の約 10 分の 1 であり，SHA-256 機能の約 2 分の 1 になっている。また，安全性についての比較を行った結果，AES 暗号化機能や SHA-256 機能を用いてパスワードの暗号化を行う場合は，総当たり攻撃の対策と辞書攻撃の対策，パスワードの盗聴の対策が可能である。しかしながら，これらの機能では暗号化されたパスワードはデバイス内に固定化されているため，パスワードが盗聴された場合，JTAG への不正アクセスが懸念される。これに対して提案法は認証ごとに認情報を更新するため，暗号化された認証データが盗聴された場合でも不正アクセスを防ぐことが可能である。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 岡本 悠，馬 竣，王 森レイ，甲斐 博，高橋 寛，清水明宏	４．巻 DC2022(64)
２．論文標題 軽量なワンタイムパスワード認証方式を用いたJTAGアクセス機構のFPGA実装と面積評価	５．発行年 2022年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 168-173
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 魏　少奇・塩谷晃平・王　森レイ・甲斐　博・樋上喜信・高橋　寛	４．巻 DC2022(87)
２．論文標題 グラフニューラルネットワークと深層強化学習による論理回路のテストポイント選択法	５．発行年 2022年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 27-32
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Senling Wang, Xihong Zhou, Yoshinobu Higami, Hiroshi Takahashi, Hiroyuki Iwata, Yoichi Maeda, Jun Matsushima	４．巻 28
２．論文標題 Test Point Insertion for Multi-Cycle Power-On Self-Test	５．発行年 2023年
３．雑誌名 ACM Transactions on Design Automation of Electronic Systems	６．最初と最後の頁 1-21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3563552	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 王シンレイ，亀山修一，高橋寛	４．巻 24
２．論文標題 JTAGのセキュリティ脅威　―攻撃の現状とその対策―	５．発行年 2021年
３．雑誌名 エレクトロニクス実装学会学会誌	６．最初と最後の頁 668-674
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Al-AWADHI Hanan T.、AONO Tomoki、WANG Senling、HIGAMI Yoshinobu、TAKAHASHI Hiroshi、IWATA Hiroyuki、MAEDA Yoichi、MATSUSHIMA Jun	4．巻 E103.D
2．論文標題 FF-Control Point Insertion (FF-CPI) to Overcome the Degradation of Fault Detection under Multi-Cycle Test for POST	5．発行年 2020年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 2289～2301
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019EDP7235	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 環　輝・王　森レイ・樋上喜信・高橋　寛・岩田浩幸・前田洋一・松嶋　潤	4．巻 DC2020-35
2．論文標題 マルチサイクルテストにおけるスキャンパターン削減指向制御ポイントの選定法	5．発行年 2020年
3．雑誌名 電子情報通信学会技術報告	6．最初と最後の頁 24-29
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 中岡典弘・王　森レイ・樋上喜信・高橋　寛・岩田浩幸・前田洋一・松嶋　潤	4．巻 DC2020-75
2．論文標題 マルチサイクルテストにおける故障検出率の推定法	5．発行年 2020年
3．雑誌名 電子情報通信学会技術報告	6．最初と最後の頁 36-41
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 青野智己，中岡典弘，周　細紅，王　森レイ，樋上喜信，高橋　寛，岩田浩幸，前田洋一，松嶋　潤	4．巻 119
2．論文標題 マルチサイクルテストにおける故障検出強化のためのテストポイント挿入法	5．発行年 2020年
3．雑誌名 電子情報通信学会技術報告	6．最初と最後の頁 19-24
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 中岡典弘，青野智己，工藤壮司，王　森レイ，樋上喜信，高橋　寛，岩田浩幸，前田洋一，松嶋　潤	４．巻 119
２．論文標題 確率ベース手法を用いたマルチサイクルテストにおけるキャプチャパターンの故障検出能力低下問題の解析	５．発行年 2019年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 145-150
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計15件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 魏少奇，王森レイ，甲斐博，樋上喜信，高橋寛
２．発表標題 グラフ畳み込みニューラルネットワークを用いたテストポイント選定について
３．学会等名 令和3年度電気・電子・情報関係学会四国支部連合大会
４．発表年 2021年

１．発表者名 王宇超，王森レイ，樋上喜信，甲斐博，高橋寛
２．発表標題 マルチサイクルテストの導入による組込自己診断の故障診断能力評価
３．学会等名 令和3年度電気・電子・情報関係学会四国支部連合大会
４．発表年 2021年

１．発表者名 神崎壽伯，王シンレイ，樋上喜信，甲斐博，高橋寛
２．発表標題 マルチサイクル機能動作による故障診断用パターン生成
３．学会等名 令和3年度電気・電子・情報関係学会四国支部連合大会
４．発表年 2021年

１．発表者名
荻田高史郎　甲斐　博・王　森レイ・高橋　寛・清水明宏

２．発表標題
シングルボードコンピュータ上でのSAS認証方式の計算時間の評価

３．学会等名
電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
馬竣 岡本悠 王森レイ 甲斐博 亀山修一　高橋寛　清水明宏

２．発表標題
JTAG 認証機構の軽量化設計について

３．学会等名
第36回エレクトロニクス実装学会春季講演大会

４．発表年
2022年

１．発表者名
環　輝・王　森レイ・樋上喜信・高橋　寛

２．発表標題
マルチサイクルテストのテスト容易化のための制御ポイント選定法

３．学会等名
令和2年度電気・電子・情報関係学会四国支部連合大会

４．発表年
2020年

１．発表者名
青野智己,王　森レイ，樋上喜信，高橋　寛

２．発表標題
マルチサイクルテストにおける故障検出低下問題の解析とその対策

３．学会等名
電気関係学会四国支部連合大会

４．発表年
2019年

１．発表者名
中岡典弘・青野智己・王　森レイ・高橋　寛・ 松嶋　潤・岩田浩幸・前田洋一

２．発表標題
ハイブリッドテストポイント挿入法のマルチサイクルテストへの適用とその性能評価

３．学会等名
電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
神崎 壽伯，王 森レイ，甲斐 博，高橋 寛

２．発表標題
マルチサイクルの機能動作による故障診断能力の向上について

３．学会等名
電気・電子・情報関係学会四国支部連合大会

４．発表年
2022年

１．発表者名
馬 竣，岡本 悠，王 森レイ，甲斐 博，亀山 修一，高橋 寛，清水 明宏

２．発表標題
SAS-L を用いた JTAG 認証システムのアクセスポートロック機能回路の設計と実装

３．学会等名
電気・電子・情報関係学会四国支部連合大会

４．発表年
2022年

１．発表者名
塩谷 晃平，魏 少奇，王 森レイ，甲斐 博，高橋 寛

２．発表標題
グラフ構造強化学習を用いたテスト検査点選定法

３．学会等名
電気・電子・情報関係学会四国支部連合大会

４．発表年
2022年

１．発表者名
中野 潤平，王 森レイ，甲斐 博，樋上 喜信，高橋 寛

２．発表標題
マルチサイクルテストによるテストパターン削減

３．学会等名
電気・電子・情報関係学会四国支部連合大会

４．発表年
2022年

１．発表者名
岡本 悠，王 森レイ，甲斐 博，高橋 寛，清水 明宏

２．発表標題
エッジデバイスにおける SAS 認証回路の設計と実装

３．学会等名
電気・電子・情報関係学会四国支部連合大会

４．発表年
2022年

１．発表者名
Shaoqi Wei, Kohei Shiotani, Senling Wang, Hiroshi Kai, Yoshinobu Higami, Hiroshi Takahashi

２．発表標題
Test Point Selection Using Deep Graph Convolutional Networks and Advantage Actor Critic (A2C) Reinforcement Learning

３．学会等名
ITC-CSCC

４．発表年
2023年

１．発表者名
高橋　寛

２．発表標題
車載システム向けのテスト容易化設計法

３．学会等名
電子情報通信学会信頼性研究会（招待講演）

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	樋上　喜信 (Higami Yoshinobu) (40304654)	愛媛大学・理工学研究科（工学系）・教授 (16301)	
研究分担者	王　森レイ (Wang Senling) (90735581)	愛媛大学・理工学研究科（工学系）・講師 (16301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関