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　２ 年　 ６ 月　 ８ 日現在

機関番号：３０１０６
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ００１７９

研究課題名（和文）自己修復機能による高速・低消費電力設計対応IPSプロセッサ開発と標的型攻撃の防御

研究課題名（英文）Development of IPS Processors for High-Speed, Low-Power Design with Self-Restoration Function and Protection of Targeted Attacks

研究代表者

佐藤　友暁（Sato, Tomoaki）

北星学園大学・経済学部・教授

研究者番号：００３３６９９２

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究の目的は，安全が担保されていないネットワーク環境下で使用する機会の多い，バッテリで駆動するスマートフォン等のモバイル機器においても適用可能であり，標的型攻撃に対処可能で検知精度が高い，ホストベースのIntrusion Prevention System (IPS)及びIntrusion Detection System (IDS)を実現することです。この目的を実現するために，本研究ではウェーブパイプラインのさらなる高速化を達成するために，自動ファイニングチューニングに必要なツールを開発しました。また，FPGA上の回路を再構成するために必要な回路転送の短縮化に関する研究を行いました。

研究成果の学術的意義や社会的意義
本研究成果の学術的意義は再構成可能なFPGAの特徴を活かしたウェーブパイプラインのファインチューニング技術が提案されたことです。さらに，エントロピー符号化による最高圧縮率を達成するための新たなアーキテクチャが提案されたことです。社会的な意義は，ネットワークのセキュリティが向上するのみならず，これらの成果は高速化つ程消費電力で動作する分野に応用できることです。例えば程消費電力で動作させなければならない機械学習などに応用することが可能です。

研究成果の概要（英文）：Mobile devices are often used in insecure network environments. Since they operate on battery power, low power consumption is required. The goal of this study is to realize host-based Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) that can be used in mobile devices, and that can cope with targeted attacks and have high detection accuracy. In order to achieve this goal, we have developed the necessary tools for automatic fine-tuning for wave-pipelines. These are indispensable for further acceleration of wave-pipelines. We have also studied the shortening of circuit transfers required to reconfigure circuits on FPGAs.

研究分野：計算機工学

キーワード：IPS　FPGA　ウェーブパイプライン　ファインチューニング　機械学習　エントロピー符号化

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

不正アクセスやコンピュータウイルスによって，情報漏えいや情報改ざんの被害が多発しています。最近においては，日本年金機構が標的型攻撃によって個人情報を流出する問題を起こしました。このような，不正アクセスやコンピュータウイルスを防ぐために，Intrusion Detection System (IDS)や IPS による監視と被害防止が不可欠です。加えて，標的型攻撃を防ぐために，これらと併用して，サンドボックスを導入する必要があります。

２．研究の目的

研究代表者は，従来の IDS と IPS の問題点を解決することを目的に，いち早く平成 14 年に再構成可能なハードウエアである Field-Programmable Gate Array (FPGA)を使用したホストベース IDS に関する研究を開始し，本研究のベースとなる論文を発表しました。FPGA を用いた設計では，高速・低消費電力化手法の選択肢は非常に限らます。ロジックレベルで設計可能であり，パイプライン動作にレジスタを必要としないウェーブパイプライン手法（以下ウェーブ化）は FPGA においても高速・低消費電力化に有効です。

ウェーブ化回路は，以下の式によって回路のクロック周期T_{CK}が求められます。

$$T_{CK} > \left(D_{MAX} - D_{MIN}\right) + T_{OV} \qquad (1)$$

(1)式から，最大遅延時間であるD_{MAX}と最小遅延時間であるD_{MIN}の差が最小になるように回路を構成することで，ウェーブ化回路は高スループットで動作します。T_{OV}は，チップ製造工程における影響，動作温度，動作電圧，クロックスキュー等の影響を考慮したオーバヘッドです。ウェーブ化回路は遅延時間の変化によって正常に動作しない問題があります。この問題はT_{OV}によって吸収させることが可能ですが，これは動作周波数を低下させる原因です。そこで，T_{OV}を最小値にする必要があります。設計時に を最小値にすることは限界があります。従って，本研究では回路動作時における自己修復技術によって T_{OV}の最小化を実現します。

次にサンドボックスエンジンは，現在の深刻な問題である標的型攻撃等を防ぐためにホストベースで実装される必要があります。例えば Java アプレットをサンドボックス内で検証する場合， Java 仮想マシンはサンドボックス内で動作させる必要があります。Java 仮想マシンを高速かつ低消費電力で動作させるために，Java アーキテクチャによる CPU が必要となります。これらは，IPS プロセッサで使用される検知回路と異なり，回路規模が大きくなる問題があります。従って，複数のサンドボックスエンジンを同時に IPS プロセッサへ搭載することは困難です。そこで，回路を再構成するための時間の削減を目的とします。

３．研究の方法

遅延時間を調整することでウェーブパイプライン処理を実現しています。ウェーブパイプラインは動作時の温度や電圧、製造時の状態が遅延時間に影響を与えます。そのため、遅延時間にマージンを加えることでこれらの影響を吸収しています。しかし、そのマージンはスループットに影響を与えます。

遅延時間を動的に調整することで、このマージンを小さくすることができます。そこで、本研究課題では自動ファインチューニングを提案しました。提案手法は以下の通りです。

1. 波線回路の設計者が波線回路に正常動作を検証するための回路を追加する。
2. その結果をもとに，経路制御用回路が最適な経路を作成する。
3. 最適化された経路は CB に組み込まれる。
4. 2 番目と 3 番目が常に繰り返される。

我々が提案してきた CB はセレクタで構成されている。そのため，Connection Block (CB)内の経路を動的に容易に変更することが可能である。本研究課題では，自動ファインチューニングに必要なツールの開発を行いました。

当初は標的型攻撃を防ぐために，サンドボックスエンジンを IPS プロセッサに搭載することを本研究の計画時に予定していましたが，機械学習の研究が発展してきた結果，標的型攻撃は機械学習によって防ぐ方法が可能になってきました。そこで，本研究ではサンドボックスエンジンや機械学習の両方においても必要とされる回路を再構成するために必要な回路転送の短縮化に関する研究を行いました。

本研究課題では、エントロピー符号の組み合わせにより最高圧縮率を求めるアーキテクチャを提案します。通常、エントロピー符号の組み合わせは、発生確率に基づいて決定されます。しかし，本アーキテクチャの特徴は，すべてのエントロピー符号の組み合わせを行い，最高の圧縮率が得られる組み合わせの符号を使用することです。

エントロピー符号化は，データ圧縮に用いられます。可逆圧縮であるため，データ通信やプロセッサでの応用が可能である。表１に示すように，エントロピー符号化の特徴は，発生確率に応じて符号長が変化することである。つまり、アプリケーションによっては、この確率が最高の圧縮率ではない場合がある。

常に最高の圧縮率を実現するために，そのためのアーキテクチャを提案します。そのアーキテクチャを図 1 に示す。このアーキテクチャの特徴は，すべての組み合わせをハードウェアレベルで処理することであす。ハードウェアで処理するということは、並列処理が可能であることを意

味します。

表１：　エントロピー符号化

Sample value	Code word (Equal length)	Occurrence probability	Code word (Variable length)
0	000	0.5	1
1	001	0.1	010
2	010	0.1	011
3	011	0.025	00011
4	100	0.025	00100
5	101	0.025	00010
6	110	0.025	00101
7	111	0.1	0011

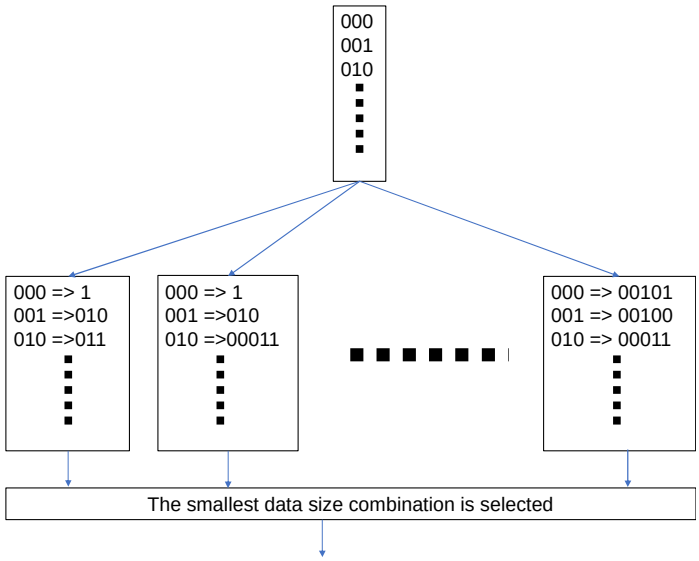


図１：最高圧縮率を実現するエントロピー符号化処理のためのアーキテクチャ

本研究に使用した開発環境は以下のとおりです。

表２：　　開発環境

OS	Cent OS 7.5 x86-64
CPU	Intel Core i7-7700K 4.2GHz
Memory	16GBytes
Logic synthesis	Synopsys Design Compiler　N-2017.09-SP1
Technology	45 nm C-MOS
Standard cell library	NanGate FreePDF45 Open Cell Library

４．研究成果

本研究では，経路解析ツールを開発し，図 2 の CB の経路解析を行いました。このツールでは，CB の入力ポートと出力ポート，セレクタとセレクタの間の経路関係を隣接関係リストで表現します。次に深さ優先探索により解析を行います。その結果を図３に示します。

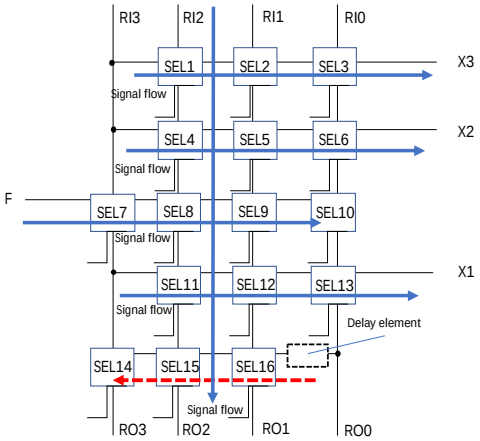
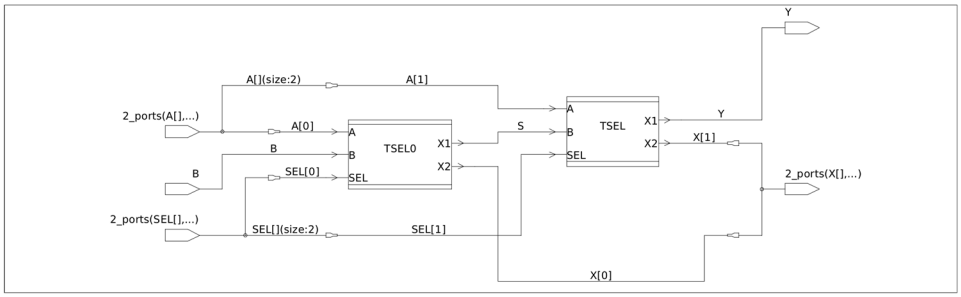


図２： Connection Block

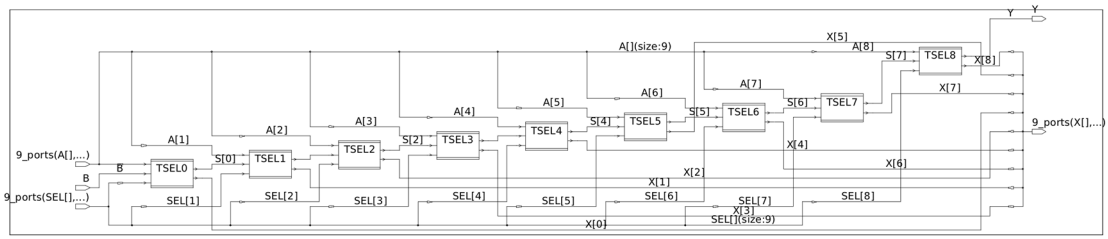
```
************************** 2, 6
[R13]=>(S1)=>(S2)=>(S3)=>[X3]  :3
************************** 2, 7
[R13]=>(S1)=>(S4)=>(S5)=>(S6)=>[X2]  :4
[R13]=>(S1)=>(S2)=>(S5)=>(S6)=>[X2]  :4
[R13]=>(S1)=>(S2)=>(S3)=>(S6)=>[X2]  :4
[R13]=>(S4)=>(S5)=>(S6)=>[X2]  :3
************************** 2, 8
[R13]=>(S7)=>(S11)=>(S12)=>(S13)=>[X1]  :4
[R13]=>(S7)=>(S8)=>(S11)=>(S12)=>(S13)=>[X1]  :5
[R13]=>(S7)=>(S8)=>(S9)=>(S12)=>(S13)=>[X1]  :5
[R13]=>(S7)=>(S8)=>(S9)=>(S10)=>(S13)=>[X1]  :5
[R13]=>(S1)=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S12)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S6)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S1)=>(S2)=>(S3)=>(S6)=>(S10)=>(S13)=>[X1]  :6
[R13]=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>[X1]  :5
[R13]=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>[X1]  :5
[R13]=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>[X1]  :5
[R13]=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>[X1]  :5
[R13]=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>[X1]  :5
[R13]=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>[X1]  :5
************************** 2, 9

途中省略


************************** 2, 11
[R13]=>(S7)=>(S11)=>(S12)=>(S16)=>[RO1]  :4
[R13]=>(S7)=>(S11)=>(S12)=>(S13)=>(S16)=>[RO1]  :5
[R13]=>(S7)=>(S8)=>(S11)=>(S12)=>(S16)=>[RO1]  :5
[R13]=>(S7)=>(S8)=>(S11)=>(S12)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S7)=>(S8)=>(S9)=>(S12)=>(S16)=>[RO1]  :5
[R13]=>(S7)=>(S8)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S7)=>(S8)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S11)=>(S12)=>(S16)=>[RO1]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S12)=>(S16)=>[RO1]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R12]=>(S1)=>(S4)=>(S5)=>(S9)=>(S12)=>(S16)=>[RO1]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S12)=>(S16)=>[RO1]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S2)=>(S5)=>(S6)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S1)=>(S2)=>(S3)=>(S6)=>(S10)=>(S13)=>(S16)=>[RO1]  :7
[R13]=>(S4)=>(S8)=>(S11)=>(S12)=>(S16)=>[RO1]  :5
[R13]=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S4)=>(S8)=>(S9)=>(S12)=>(S16)=>[RO1]  :5
[R13]=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S4)=>(S5)=>(S9)=>(S12)=>(S16)=>[RO1]  :5
[R13]=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>(S16)=>[RO1]  :6
[R13]=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>(S16)=>[RO1]  :6
************************** 2, 12
[R13]=>(S7)=>(S11)=>(S12)=>(S13)=>[RO0]  :4
[R13]=>(S7)=>(S8)=>(S11)=>(S12)=>(S13)=>[RO0]  :5
[R13]=>(S7)=>(S8)=>(S9)=>(S12)=>(S13)=>[RO0]  :5
[R13]=>(S7)=>(S8)=>(S9)=>(S10)=>(S13)=>[RO0]  :5
[R13]=>(S1)=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S12)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S9)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S2)=>(S5)=>(S6)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S1)=>(S2)=>(S3)=>(S6)=>(S10)=>(S13)=>[RO0]  :6
[R13]=>(S4)=>(S8)=>(S11)=>(S12)=>(S13)=>[RO0]  :5
[R13]=>(S4)=>(S8)=>(S9)=>(S12)=>(S13)=>[RO0]  :5
[R13]=>(S4)=>(S8)=>(S9)=>(S10)=>(S13)=>[RO0]  :5
[R13]=>(S4)=>(S5)=>(S9)=>(S12)=>(S13)=>[RO0]  :5
[R13]=>(S4)=>(S5)=>(S9)=>(S10)=>(S13)=>[RO0]  :5
[R13]=>(S4)=>(S5)=>(S6)=>(S10)=>(S13)=>[RO0]  :5
```

図３：図２の R13 **からの解析結果**

ファインチューニングのための遅延時間解析ツールを開発するために必要な配線経路の遅延時間を解析する。　フリーの 45nm **ライブラリを使用し，経路解析用の配線経路モデルを設計した。　モデルの遅延時間はシノプシス社の** Design Compiler **を用いて解析している。**
表 2 **の開発環境を用いて，経路解析用の配線パスモデルを設計する。そのモデルを図** 3 **に示す。図２のＣＢとＳＢはセレクタで構成されているので、図３に示すように，セレクタはセレクタで構成されている。図** 3 **に示すようにセレクタを直列に配置し遅延時間を解析する。また，図３**(b)**の回路について遅延時間，面積，消費電力を解析した結果を図３に示します。この結果をもとにファインチューニングのためのツールが開発されました。**
図４に開発されたエントロピー符号化処理のための論理合成結果をしまします。



(a)



(b)

図 3: **遅延時間解析モデルのための論理合成結果** (a) **セレクタ数が２の場合** (b) **セレクタ数が** 9 **の場合**

No. of selectors	Delay time (ns)	Area	Total dynamic Power (nW)	Cell leakage Power (nW)
1	0.07	1.862	519.66	35.93
2	0.14	3.724	1227.1	71.85
3	0.21	5.586	1969.3	107.69
4	0.28	7.448	2748.9	143.7338
5	0.35	9.31	3542.4	179.5593
6	0.41	11.172	4282.2	215.3313
7	0.48	13.034	5041.6	251.53
8	0.55	14.896	5846.2	287.79
9	0.62	16.758	6697.5	323.53

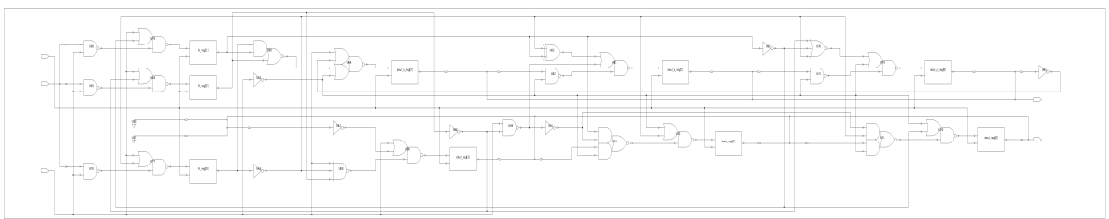


図４： エントロピー符号化処理のための回路

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　9件／うちオープンアクセス　1件）

１．著者名 T. Sato, S. Chivapreecha, K. Higuchi and P. Moungnoul	４．巻
２．論文標題 Designing a Fine-Tuning Tool for Machine Learning with High-Speed and Low-Power Processing	５．発行年 2018年
３．雑誌名 Proc. of ISCIT 2018	６．最初と最後の頁 204-207
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 該当する

１．著者名 T. Sato, S. Chivapreecha, K. Higuchi and P. Moungnoul	４．巻
２．論文標題 Automatc Fine-Tuning of Wave-Pipelined Circuits and Development of Route Analysis Tool for It	５．発行年 2018年
３．雑誌名 Proc. of ITC-CSCC 2018	６．最初と最後の頁 118-121
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 該当する

１．著者名 T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi	４．巻 11
２．論文標題 RCA on FPGAs Designed by the RTL Design Methodology and Wave-Pipelined Operation	５．発行年 2017年
３．雑誌名 ECTI Transactions CIT	６．最初と最後の頁 11-20
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 オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi	４．巻
２．論文標題 A Circuit Design for IEEE 802.11ac by ASIC-FPGA Co-Design	５．発行年 2017年
３．雑誌名 Proc. of ISMAC 2017	６．最初と最後の頁 89-92
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 該当する

1．著者名 T. Sato, S. Chivapreecha, K. Higuchi and P. Moungnoul	4．巻
2．論文標題 A Detection Method of Web Authentication Problems for Mobile Devices Corresponding to IEEE 802.11ac	5．発行年 2018年
3．雑誌名 Proc. of IWAIT 2018	6．最初と最後の頁 221.1-221.4
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 該当する

1．著者名 T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi	4．巻 2
2．論文標題 Throughput of a Firewall Unit on FPGAs developed by the RTL Design Methodology	5．発行年 2017年
3．雑誌名 Proc. of iEECON 2017	6．最初と最後の頁 423-426
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 該当する

1．著者名 T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi	4．巻 -
2．論文標題 An FPGA Architecture for ASIC-FPGA Co-Design to Streamline Processing of IDSs	5．発行年 2016年
3．雑誌名 Proc. of CTS 2016	6．最初と最後の頁 412-417
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CTS.2016.0079	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 該当する

1．著者名 T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi	4．巻 -
2．論文標題 Designing a Firewall Unit on the FPGA Composed of Selectors	5．発行年 2016年
3．雑誌名 Proc. of SISA 21016	6．最初と最後の頁 53-58
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 該当する

１．著者名 T. Sato, S. Chivapreecha, K. Higuchi and P. Moungnoul	４．巻 -
２．論文標題 Proposal of a High-speed and Low-power Architecture for Entropy Coding Processing to Achieve Highest Compression Rate	５．発行年 2019年
３．雑誌名 Proc. of the 1st ECTI UEC Workshop on AI and Applications	６．最初と最後の頁 72-73
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 該当する

〔学会発表〕　計0件

〔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