

科学研究費助成事業 研究成果報告書

平成 29 年 6 月 6 日現在

機関番号：11101

研究種目：基盤研究(C) (一般)

研究期間：2013～2016

課題番号：25330149

研究課題名(和文) 配線による遅延調整手法を用いたホストベースIPSプロセッサの開発と検知回路最適化

研究課題名(英文) Development of Host-Based IPS Processor Using Delay Adjustment Method by Routing and Optimization of Detection Circuits

研究代表者

佐藤 友暁 (Sato, Tomoaki)

弘前大学・総合情報処理センター・准教授

研究者番号：00336992

交付決定額(研究期間全体)：(直接経費) 3,700,000円

研究成果の概要(和文)：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る。実際に日本年金機構は標的型攻撃によって個人情報を流出する問題を起こした。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、IDS(不正アクセス検知システム)やIPS(不正アクセス防御システム)による監視と被害防止が不可欠である。本研究ではモバイル機器においてこれらの問題に技術的なアプローチで解決することを目的として、ウェーブパイプライン手法のファインチューニングを再構成可能なプロセッサ上で実現できることを明らかにした。加えて検知回路の最適化をASIC-FPGA協調設計によって実現した。

研究成果の概要(英文)：Unauthorized access and computer viruses cause problems with information leakage and tampering. Actually, a targeted attack made leakage of personal information in Japan Pension Service. In order to avoid unauthorized access and computer viruses, Intrusion Detection Systems (IDSs) or Intrusion Prevention Systems (IPSs) should be used. In this study, it is clarified that a fine-tuning method for wave-pipelining can be realized on reconfigurable hardware for the purpose of addressing these problems with a technical approach in mobile devices. In addition, the optimization of the detection circuit was realized by ASIC-FPGA co-design.

研究分野：計算機工学

キーワード：IDS IPS FPGA RTL ウェーブパイプライン

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る。研究開始前年においては、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(Intrusion Prevention System)による監視と被害防止が不可欠である。

特にスマートフォンやモバイル PC (Personal Computer)においては CPU の処理能力が低く、CPU 負荷の高いパケットレベルでの詳細な解析や高精度のアノマリ検知は不可能である。バッテリーによる低消費電力動作が要求されるスマートフォンやタブレット PC の普及によって、ホストベース IDS と IPS の機能的な問題点の解消はより困難になる。

2. 研究の目的

本研究の目的は、多様なネットワーク環境下で使用されるスマートフォンやモバイル PC においても適用可能であり、検知精度が高く、高速・低消費電力、省スペースで動作するホストベース IPS を実現することである。そのために不可欠である検知回路のウェーブパイプライン化設計において、再構成可能なハードウェアの特徴を生かし、動作検証後に配線経路の遅延時間調整により、さらなる高速化を実現することである。

3. 研究の方法

(1) ウェーブパイプラインのファインチューニング回路の開発

本研究では、ウェーブパイプライン設計におけるファインチューニングを論理回路構成後において実現可能にする。高速・低消費電力で動作する IPS プロセッサの実現は、FPGA (Field-Programmable Gate Array)の使用が不可欠である。FPGA 上に構築される回路トランジスタレベルで設計することができないため、高速・低消費電力化設計手法は制限される問題がある。

FPGA 上の回路において高速・低消費電力化が実現する方法の一つとして、ウェーブパイプライン設計を用いることである。この設計でさらなる高スループットを達成するためには、ファインチューニングを行うことである。これまでのウェーブパイプライン設計では、ファインチューニングはトランジスタレベルでの設計でのみ実現され、FPGA 上の回路では実現されてなかった。

FPGA 上の回路でファインチューニングを実現するために、論理回路構成後にファインチューニングを実現させるための接続ブロックを図1に提案する。図2に図1で使用されている配線制御のために使用されているスイッチを示す。このFPGAは接続ブロック、図3に示すスイッチブロック、図4に示すロジックブロックで構成されてい

る。

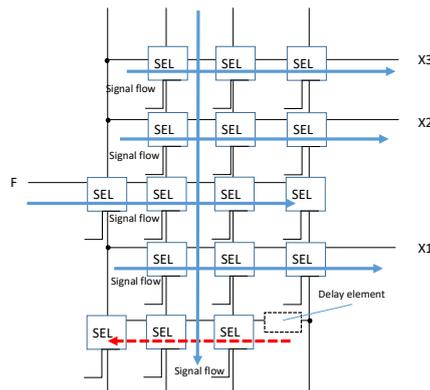


図1 ファインチューニング向け接続ブロック

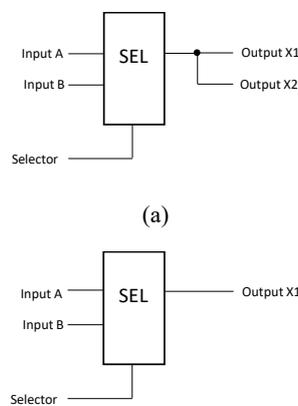


図2 RTL 設計向け配線スイッチ (a) 2入力2出力 (b) 2入力1出力

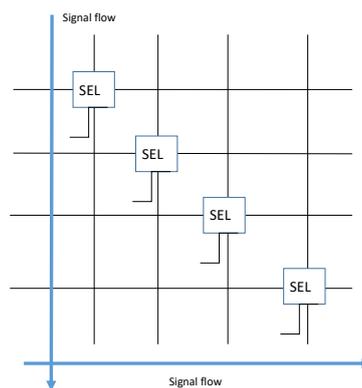


図3 スイッチブロック

(2) ASIC-FPGA 協調設計

本研究では IPS プロセッサの開発時間の短縮を目的として RTL (Register Transfer Level) で FPGA の開発が行われた。また不正アクセス検知回路と異なり、CPU (Central Processing

Unit)等はチップ製造後に変更する必要がない。このような場合は FPGA での回路よりも ASIC (Application Specific Integrated Circuit)で開発することによって FPGA 上の回路より大幅なスループット向上や消費電力削減が達成可能である。

図1のブロックは遅延時間が増加する問題があるため、図5に示す通常型の接続ブロックを開発し、これを組み込んだFPGAの開発を行った。このFPGAを使用してASIC-FPGA 協調設計による加算回路を設計した。この加算回路は図6に示される。

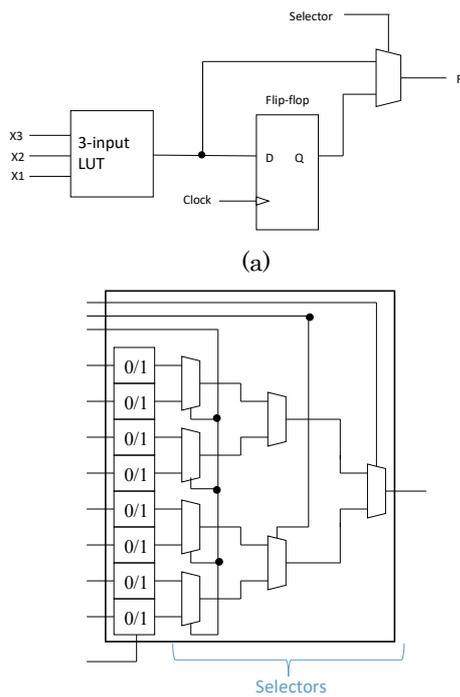


図4 ロジックブロック (a)ロジックブロックの構成 (b) LUT

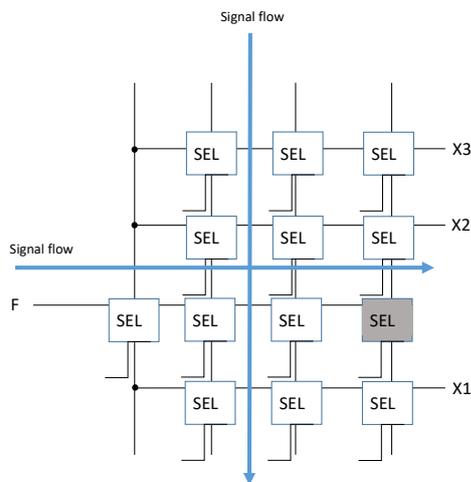


図5 通常型接続ブロック

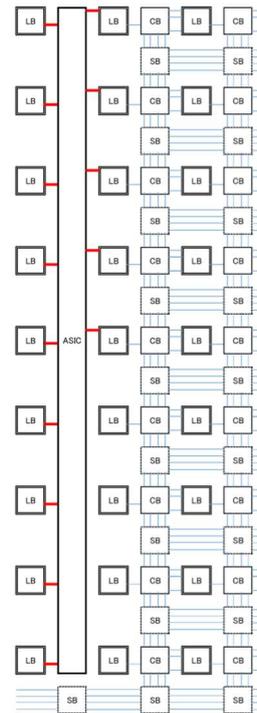


図6 ASIC-FPGA 協調設計による加算回路

4. 研究成果

(1) ウェーブパイプラインのファインチューニング回路の評価結果

図1の回路の遅延時間解析結果は、表1に示される。この結果より7段階で遅延時間の調整が可能になることが明らかになった。

表1 遅延時間解析結果

Number of passed selectors	Input port	Output port	Route	Delay time	Delay time difference
2	F	R(3)	SEL1 -> SEL8	0.53 ns	0.00 ns
3	F	R(2)	SEL1 -> SEL3 -> SEL7	0.91 ns	0.38 ns
4	F	R(3)	SEL1 -> SEL3 -> SEL7 -> SEL8	1.08 ns	0.17 ns
5	F	R(3)	SEL1 -> SEL2 -> SEL3 -> SEL7 -> SEL8	1.36 ns	0.28 ns
6	F	R(3)	SEL1 -> SEL3 -> SEL4 -> SEL6 -> SEL7 -> SEL8	1.63 ns	0.27 ns
7	F	R(3)	SEL1 -> SEL3 -> SEL4 -> SEL5 -> SEL6 -> SEL7 -> SEL8	2.00 ns	0.37 ns
8	F	R(3)	SEL1 -> SEL2 -> SEL3 -> SEL4 -> SEL5 -> SEL6 -> SEL7 -> SEL8	2.39 ns	0.39 ns

すなわち、図 1 の回路は FPGA 上の回路のウェーブパイプライン化において、ファインチューニングが可能になることが明らかにされた。加えて、これは FPGA であるため、動作検証後のファインチューニングが実現することも明らかになった。図 7 に示す、最小遅延時間と最大遅延時間が実現できることを明らかにされた。

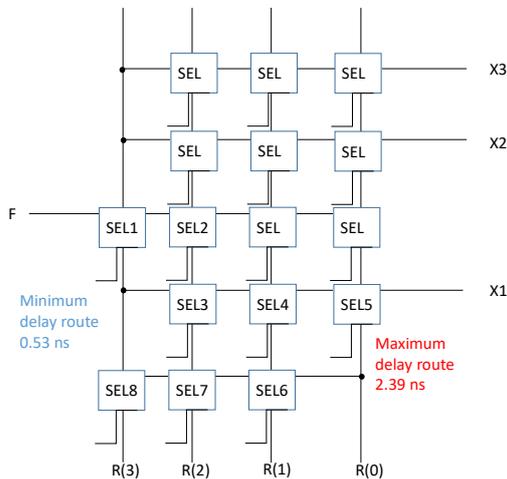


図 7 コネクションブロックの最大遅延時間と最小遅延時間

(2) ASIC-FPGA 協調設計の評価結果

図 8 に ASIC-FPGA 協調設計による加算回路のスループットの評価結果を示す。この結果より、4 ビットの加算回路においては、提案した FPGA や本研究で使用した 0.18 μ C-MOS テクノロジーで開発されている商用の CPLD と

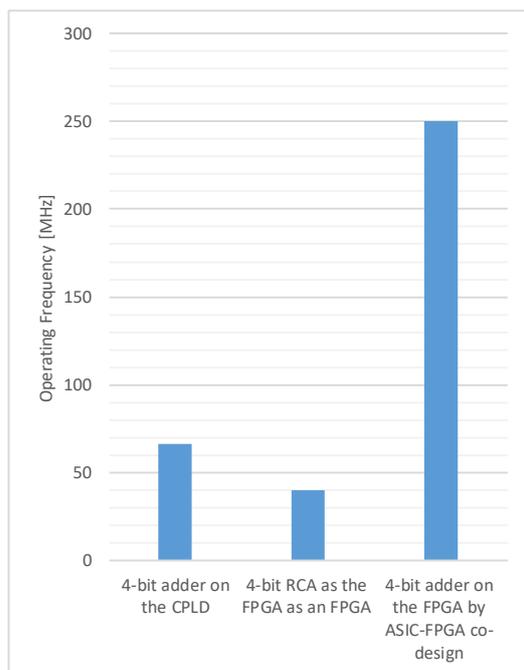


図 8 4 ビット加算回路のスループット

比較された。その結果、大幅なスループット向上が可能であることが明らかにされた。

図 9 において、加算回路のワード幅と遅延時間の関係が明らかにされた。この結果より、ASIC-FPGA 協調設計による加算回路はワード幅に依存せず完全に ASIC で開発された加算器に比較して若干の遅延時間の増加のみで実現されることが明らかになった。また 50 ビットを超えるあたりから、CPLD の遅延時間が他の二つより小さくなっている。これは論理合成を行う際に、最適化オプションを使用しなかったためである。今後の課題として、最適化オプションを使用しているの評価があげられる。

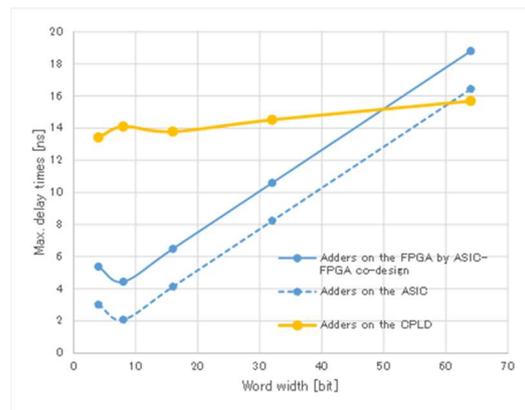


図 9 加算回路のワード幅と遅延時間の関係

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 15 件)

- ① T. Sato, S. Chivapreecha and P. Moungnoul, "A Logic Block for Wave-Pipelining," Proc. of IMETI 2013, pp. 130-134, 2013. 査読有
- ② T. Sato, P. Moungnoul, S. Chivapreecha and K. Higuchi, "Performance Estimates of an Embedded CPU for High-Speed Packet Processing," Proc. of ECTI-CON 2014, pp.1298.1-1298-5, 2014. 査読有
- ③ T. Sato, S. Chivapreecha and P. Moungnoul, "Evaluation of Logic Blocks for Reconfigurable Wave-Pipelined Circuits with 45nm CMOS Technology," Proc. of ITC-CSCC2014, pp. 464-465, 2014. 査読有
- ④ T. Sato, S. Chivapreecha and P. Moungnoul, "Design and Analysis of Crossbar Switch Circuits for Reconfigurable Wave-Pipelined Circuits," Proc. of CreTech 2014, pp. 12-15, 2014. 査読有

- ⑤ T. Sato, S. Chivapreecha and P. Moungnoul, "Wiring Control by RTL Design for Reconfigurable Wave-Pipelined Circuits," Proc. of APSIPA ASC 2014, pp. WP1-3-1-WP1-3-6, 2014. 査読有
- ⑥ T. Sato, S. Chivapreecha and P. Moungnoul, "A Crossbar Switch Circuit Design for Reconfigurable Wave-Pipelined Circuits," Proc. of WMSCI 2014, vol. II, pp. 200-205, 2014. 査読有
- ⑦ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "Evaluations of Waved-Shift Registers for Multiplexed Bus," Proc. of iEECON2014, pp. 109.1-109.4, 2014. 査読有
- ⑧ T. Sato, S. Chivapreecha and P. Moungnoul, "The Potential of Routes Configured with the Switch Matrix by RTL," Applied Mechanics and Materials Journal, vol. 781, pp. 189-192, 2015. 査読有
- ⑨ T. Sato, S. Chivapreecha and P. Moungnoul, "Fine-Tuning of Wave-Pipelines on FPGAs Developed by the RTL Design," Proc. of ECTI-CON 21015, pp. 1230.1-1230.6, 2015. 査読有
- ⑩ T. Sato, S. Chivapreecha and P. Moungnoul and K. Higuchi "Proposal of the security log collection method of public Wi-Fi services on private IPv4 address spaces utilizing Raspberry Pi," Proc. of ICESIT 2015, pp. 6-7, 2015. 査読有
- ⑪ T. Sato, S. Chivapreecha and P. Moungnoul, "A Connection Block Implemented in the RTL Design for Delay Time Equalization of Wave-Pipelining," Journal of Systemics, Cybernetics and Informatics, vol. 14, no. 1, pp. 49-54, 2016. 査読有
- ⑫ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "Designing a Firewall Unit on the FPGA Composed of Selectors," Proc. of SISA 21016, pp. 53-58, 2016. 査読有
- ⑬ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "An FPGA Architecture for ASIC-FPGA Co-Design to Streamline Processing of IDSs," Proc. of CTS 2016, pp. 412-417, Oct. 2016. 査読有
- ⑭ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "Throughput of a Firewall Unit on FPGAs developed by the RTL Design Methodology," Proc. of iEECON 2017, vol. 2, pp. 423-426, 2017. 査読有

- ⑮ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "RCA on FPGAs Designed by the RTL Design Methodology and Wave-Pipelined Operation, ECTI Transactions CIT, vol. 11, no. 1, pp. 11-20, 2017. 査読有

[学会発表] (計 3 件)

- ① T. Sato, S. Chivapreecha and P. Moungnoul, "The Potential of Routes Configured with the Switch Matrix by RTL," iEECON 2015, Mar. 2015.
- ② T. Sato, S. Chivapreecha and P. Moungnoul, "A Connection Block Implemented in the RTL Design for Delay Time Equalization of Wave-Pipelining," WMSCI 2015, Jul. 2015.
- ③ T. Sato, S. Chivapreecha, P. Moungnoul and K. Higuchi, "RCA on FPGAs Designed by the RTL Design Methodology and Wave-Pipelined Operatio, ECTI-CON 2016, Jun. 2016.

[図書] (計 件)

[産業財産権]

○出願状況 (計 件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況 (計 件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

[その他]
ホームページ等

6. 研究組織

(1)研究代表者

佐藤 友暁 (SATO TOMOAKI)

弘前大学・総合情報処理センター・准教授

研究者番号：00336992

(2)研究分担者

()

研究者番号：

(3)連携研究者 ()

研究者番号：

(4)研究協力者 ()