様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　１８　日現在

機関番号：　１３９０４
研究種目：　基盤研究(C)
研究期間：　2011～2014
課題番号：　２３５００００６１

研究課題名（和文）専用回路技術によるモデル予測制御の高速化

研究課題名（英文）Performance improvement of Model Predictive Control by custom computing circuitry

研究代表者
市川　周一（Ichikawa, Shuichi）

豊橋技術科学大学・工学（系）研究科（研究院）・教授

研究者番号：７０２６２８５５

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：近年の制御技術の発達により制御性能は著しく改善されたが，必要な計算量も増大した．申請者は制御応用に専用回路技術を適用し，高性能な実時間制御を実現する研究を進めてきた．本研究ではモデル予測制御のハードウェア化を研究目標とした．演算回路の高速化については，ハードウェア特殊化した暗号回路，SHA-3ハッシュ回路の高速実装，鍵依存AES回路の消費電力評価，Modular乗算回路，BLAKE-256ハッシュ回路等を検討した．制御論理の知的所有権保護について企業から要望されたため，ハードウェア化による高秘匿性制御論理についても研究した．

研究成果の概要（英文）：Recent progresses in control theory resulted in better control precision in exchange for a substantial increase of calculation cost. This researcher has been working on the application of custom computing circuitry to control applications for high-performance real-time control systems. In this research, high-performance arithmetic circuits were investigated; e.g., key-specific encryption circuit, improved hash circuit, the power consumption of key-specific AES circuit, modular multiplication circuit, etc. Inspired by a request from commercial control vendors, secure control logic designs were also investigated to protect intellectual property of various control systems.

研究分野：　計算機科学

キーワード：　制御論理　ハードウェア特殊化　知的所有権保護　セキュアプロセッサ

１．研究開始当初の背景

制御技術は，家電製品から自動車・航空機・人工衛星に至るまで，あらゆる工業製品に不可欠の技術である．近年の制御技術の発達により制御性能は著しく改善されたが，それと同時に必要な計算量も増大した．特に実時間制御が必要な組込みシステムにおいては，計算時間の増加が深刻な問題となっている．そこで近年注目されているのが，制御論理のハードウェア化による高速化である．

申請者は，制御応用に専用回路技術を適用し，高性能な実時間制御を実現する研究を進めてきた．以下に 2 つの例を挙げる．

(1) PLC (Programmable Logic Controller) は制御用計算機として広く用いられているが, その性能は高いとは言えない. PLC 命令列からハードウェア記述を自動生成し, 論理回路として実現することにより, PLC の 184～8050 倍の性能が得られた. 制御用 FPGA ボードを開発し，企業と共同開発した産業用機械で動作を確認した.

(2) 制振制御応用の Simulink モデルを HDL に変換し，FPGA 上で実装評価した．制振制御と予測制御を導入した搬送システムを FPGA 上で実装した結果，ソフトウェア(1.6 GHz Atom)の 20～100 倍程度の性能が得られた．

２．研究の目的

本研究では，モデル予測制御(MPC; Model Predictive Control)のハードウェア化について検討する．MPC は制御対象の動的モデルに基づいて制御出力を決定する高度制御方式で，制御品質は向上するが計算量が増大するという特徴がある．

MPC は制約を考慮した最適化問題という側面を持ち，扱う制約や方法論により様々なサブカテゴリに分かれている．本研究では，対象をシステム同定により線形化し，多変数制御問題を最小二乗問題として定式化した後，後退ホライズン方策を用いて制御周期毎に実時間で二次計画法(QP)問題を解く手法について検討する．

本研究の目的は，以下の通りである．

(1) MPC を専用ハードウェアで実現するための高速化技術を検討する．

(2) MPC で用いる実時間 QP 求解器の設計・実装・評価を行う．

３．研究の方法

研究は，以下の 3 つのステップで行う．

(1) 企業に協力を要請し，評価対象とする MPC の実例と典型例を収集し，ハードウェア化の効果が大きい応用を選択する．

(2) MPC の核となる二次計画法（QP）の解を求めるハードウェアの構成を検討する．

(3) QP 求解器で用いる演算器について，最適なデータ表現やアルゴリズムを検討する．

４．研究成果

現実の制御応用を分析するため，幾つかの企業に働きかけて情報収集を行った．特に，JFE エンジニアリングとは 2 年間にわたり共同研究を行って，実社会の制御システムと PLC プログラムの分析を行うことができた[1][2]. その詳細は守秘義務のため明らかにできないが，共同研究の分析結果はその後の学会発表の基礎データとして活用した（宇山・藤枝・市川 2013～2015）.

上記共同研究の中で，制御プログラムのハードウェア化により知的所有権を守ることの重要性が企業側から指摘された．そこで当初の研究目的（制御の高速化）に加えて，知的所有権保護（制御のセキュリティ向上）を研究目的に加えた．

PLC 命令列（ラダープログラム）をハードウェア記述に変換し，FPGA 上で実装することは，過去の研究で実現済である[3]．そこで本研究では，ソフトウェアの難読化手法を論理回路に適用して，制御論理の分析を妨げる手法について検討した．

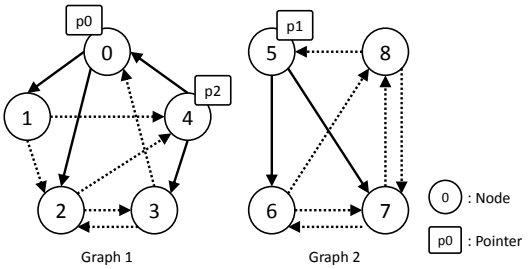
Collberg らは Opaque Predicates と呼ばれる手法を提案し，解析困難な状態遷移をソフトウェアに組み入れることで，ソフトウェアの解析を妨げる手法を提案した．われわれは，Opaque Predicates を論理回路に適用し，生成される制御ハードウェアが難読化されることと，その副作用（論理規模増大・動作速度低下）がわずかであることを実証した．（宇山・藤枝・市川 2015）

---

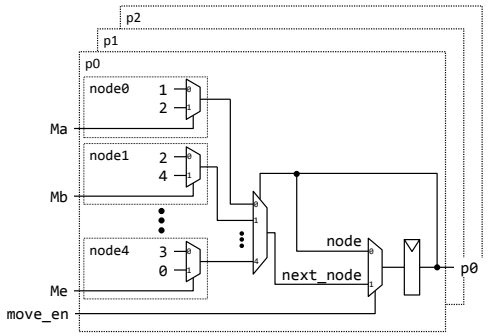
[1] "PLC プログラムの FPGA ハードウェア記述言語化に関する実機化検討," JFE エンジニアリング, 受託研究, 平成 24 年 6 月 1 日～平成 25 年 2 月末日

[2] "PLC プログラムの FPGA ハードウェア記述言語化に関する基本検討," JFE エンジニアリング, 受託研究, 平成 23 年 6 月 28 日～9 月 30 日

[3] S.Ichikawa et al. “An FPGA implementation of hard-wired sequence control system based on PLC software," IEEJ Transactions on Electrical and Electronic Engineering, Vol. 6, No. 4, pp. 367--375 (2011).



図：Colleberg らの提案手法



図：宇山・藤枝・市川による実現方法

当初計画に含まれる「演算回路の高速化」についても各種応用で検討を進めた．ハードウェア特殊化を暗号回路に適用（松岡，日野，市川 2011），SHA-3 ハッシュ回路の高速実装（鮎沢・藤枝，市川 2014），鍵依存 AES 回路の消費電力評価（松岡，市川 2012），Modular 乗算回路（田村, 山田, 市川 2012），BLAKE-256 ハッシュ回路（Syafiq, Ichikawa 2011），など枚挙に暇が無いが，詳細については紙数の関係上省略する．

これ以外にも，幾つかの派生テーマについて研究成果が得られたので以下に簡単にまとめる．

制御システム・組込みシステムの知的財産権を保護するために，PLC あるいは組込みプロセッサを拡張してセキュリティを高める手法も検討した．本研究者はこれまでも「プロセッサ多様化」に基づくセキュアプロセッサについて研究してきた[4]．本研究では，低消費電力化技術である IRF (Instruction Register File)を利用してプロセッサ多様化を実現する手法について研究・評価した．（藤枝・市川 2015）

本研究の目的は計算量の多い制御アルゴリズムの高速化であるが，実応用を検討してゆく中で，画像処理等の前処理でも計算時間が問題になっていることが判ってきた．そこでバイラテラルフィルタを用いた適応型画像処理についても研究を行った．適切なパラメータ推定により画像処理の品質を改善することができたが（真喜志，佐渡山，山田，荻野，市川 2015），計算時間が 2 時間以上かかる．現在は，処理方法の工夫と専用回路技術の適用により計算時間を短縮する手法を研究中である．

多くの制御応用で位置測定（測位）は重要であるが, 衛星を利用する GPS は屋内での使用が難しい．そこで超音波を利用した屋内測位システムが検討されている．我々は，複数周波数の超音波をアナログ回路で処理することにより，安価なセンサーとマイコンだけで実時間測位できるシステムを提案した（松岡・藤枝・市川・川口 2014）．現在は超音波発音体の設置場所に制約を設けることで高速処理を実現しているが（篠原, 坂口, 松岡, 市川，藤枝，川口 2015），制約を設けない場合あるいは高精度な測位が必要な場合は専用回路による高速化を検討する必要がある．本件については現在も引き続き研究を続けている．

[4] S.Ichikawa et al. "Diversification of Processors Based on Redundancy in Instruction Set," IEICE Transactions on Fundamentals, Vol. E91-A, No.1, pp. 211--220 (2008).

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５件）

[1] Naoki Fujieda, Shuichi Ichikawa: "An XOR-based Parameterization for Instruction Register Files," IEEJ Transactions on Electrical and Electronic Engineering, (to appear) (2015). DOI: 10.1002/tee.22123

[2] 真喜志泰希, 山田親稔, 荻野正, 市川周一: "分布間距離を用いた Bilateral Filter のパラメータ推定法の一考察," 電気学会論文誌 D, vol. 135, no. 2, pp. 87--92 (2015). DOI: 10.1541/ieejias.135.87

[3] 佐渡山史矢, 山田親稔, 市川周一, 荻野正: "単一画像を用いた再構成型超解像合成手法の検討," 電気学会論文誌 D, vol. 135, no. 2, pp. 81--86 (2015). DOI: 10.1541/ieejias.135.81

[4] Hisashi Hata, Shuichi Ichikawa: "FPGA Implementation of Metastability-based True Random Number Generator," IEICE Transactions on Information and Systems, Vol. E95-D, No. 2, pp. 426--436 (2012). DOI: 10.1587/transinf.E95.D.426

[5] 松岡俊佑, 日野善規, 市川周一: "AES 暗号と Camellia 暗号に対する暗号鍵を固定したハードウェア特殊化回路," 電子情報通信学会論文誌 D, Vol. J94-D, No. 10, pp. 1696-1700 (2011). http://search.ieice.org/bin/summary.php?id=j94-d_10_1696&category=D&year=2011&lang=J

〔国際会議発表〕（計８件）

[1] Shunsuke Matsuoka, Naoki Fujieda, Shuichi Ichikawa: "S-Box Absorption Design for Key-SpeCific AES circuits," Proc. International Conference of Global Network

for Innovative Technology (IGNITE2014), pp. 316--319 (2014).
[2] Yusuke Ayuzawa, Naoki Fujieda, Shuichi Ichikawa: "Design Trade-offs in SHA-3 Multi-Message Hashing on FPGAs," Proc. IEEE TENCON 2014 (2014). DOI: 10.1109/TENCON.2014.7022311
[3] Taiki Makishi, Shuichi Ichikawa, Tadashi Ogino, Chikatoshi Yamada: "An Efficient Estimation Parameter Method of Bilateral Filter Using Distribution Distance," Proc. IEEE TENCON 2014 (2014). DOI: 10.1109/TENCON.2014.7022331
[4] Naoki Fujieda, Shuichi Ichikawa: "Enhanced Instruction Register Files for Embedded Software Obfuscation," Proceedings of the 29th International Conference on Computers and Their Applications (CATA-2014), pp.153--158 (2014). (Best Paper Award Finalist) http://www.proceedings.com/22214.html
[5] Naoki Fujieda, Shuichi Ichikawa: "An XOR-based approach to merging entries for instruction register files," Proceedings of First International Symposium on Computing and Networking (CANDAR 2013), pp. 332--337 (2013). DOI: 10.1109/CANDAR.2013.60
[6] Shunsuke Matsuoka, Shuichi Ichikawa: "Reduction of Power Consumption in Key-specific AES circuits," Proceedings of the Third International Conference on Networking and Computing (ICNC 2012), pp. 323--325 (2012). DOI: 10.1109/ICNC.2012.61
[7] Satoru Tamura, Chikatoshi Yamada, Shuichi Ichikawa: "Implementation and Evaluation of Modular Multiplication Based on Coarsely Integrated Operand Scanning," Proceedings of the Third International Conference on Networking and Computing (ICNC 2012), pp. 334--335 (2012). DOI: 10.1109/ICNC.2012.65
[8] Muh Syafiq Irsyadi, Shuichi Ichikawa: "Two Hardware Designs of BLAKE-256 Based on Final Round Tweak," Proceedings of the 2011 IEEE Region 10 Conference (TENCON 2011), pp. 350--354 (2011). DOI: 10.1109/TENCON.2011.6129082

〔学会発表〕（計２０件）

[1] 佐藤清広, 藤枝直輝, 松岡俊佑, 市川周一, 命令拒否レジスタファイルを用いたソフトウェア改ざん攻撃への対策に関する研究, 電子情報通信学会 2015 年総合大会, D-6-1, 2015, 3, 立命館大学 びわこ・くさつキャンパス
[2] 坂口雄輝, 松岡俊佑, 藤枝直輝, 市川周一, 川口秀樹, 超音波を用いた位置測定システムの改良, 電子情報通信学会 2015 年総合大会, D-6-15, 2015, 3, 立命館大学 びわこ・くさつキャンパス
[3] 篠原巧, 松岡俊佑, 藤枝直輝, 市川周一, 川口秀樹, 超音波測位システムにおける位置計算プログラムの改良, 電子情報通信学会 2015 年総合大会, D-6-16, 2015, 3, 立命館大学 びわこ・くさつキャンパス
[4] 宇山和輝, 藤枝直輝, 市川周一, PLC 命令列のハードウェア化と Opaque Predicates による難読化の検討, 電子情報通信学会技術研究報告 CPSY/RECONF, vol.114, no.427, 221-226, 2015, 1, 慶応大学日吉キャンパス
[5] 松岡俊佑, 藤枝直輝, 市川周一, 川口秀樹, 超音波を用いたリアルタイム位置測位システムの開発, 第 23 回 MAGDA コンファレンス in 高松 (MAGDA 2014), PS35, 2014, 12, 高松
[6] 宇山和輝, 藤枝直輝, 市川周一, PLC 命令列のハードウェア変換と秘匿化手法の検討, 第 6 回 メニーコア・アーキテクチャ研究会, , 2014, 9, 御殿場
[7] 石垣良樹, 藤枝直輝, 市川周一, 行列積を計算するコプロセッサの試作, 第 6 回 メニーコア・アーキテクチャ研究会, , 2014, 9, 御殿場
[8] 松岡 俊佑, 藤枝 直輝, 市川 周一, 鍵スケジューラを省略した AES 暗号回路の FPGA による実装評価, 第 13 回情報科学技術フォーラム (FIT 2014), C-020, 2014, 9, 筑波大学
[9] 板垣佑哉, 藤枝直輝, 市川周一, PLC 命令列を C 言語に変換するツールの検討と試作, 平成 26 年度電気・電子・情報関係学会東海支部連合大会, L5-5 , 2014, 9, 中京大学, 名古屋
[10] 藤枝直輝, 宇山和輝, 市川周一, ソフトプロセッサ向けの SIMD 整数演算ユニットの設計と実装, 情報処理学会研究報告 2014-ARC-208(14), 1--4, 2014, 1, 東京工業大学
[11] 田中佑, 藤枝直輝, 市川周一, 耐タンパー性向上のための命令メモリ暗号化手法の評価, 電子情報通信学会 2014 年総合大会, D-6-7, 2014, 3, 新潟大学
[12] 鮎澤勇介, 藤枝直輝, 市川周一, セキュアハッシュ関数 SHA-3 のパイプライン回路実装と性能評価, 電子情報通信学会 2014 年総合大会, D-6-8, 2014, 3, 新潟大学
[13] 宇山 和輝, 藤枝 直輝, 市川 周一, PLC 命令列のハードウェア化における高秘匿化手法の検討, 第 5 回 メニーコア・アーキテクチャ研究会, , 2013, 9, 御殿場
[14] 鮎澤 勇介, 藤枝 直輝, 市川 周一, SHA-3 のパイプライン実装, 第 5 回 メニーコア・アーキテクチャ研究会, , 2013, 9, 御殿場
[15] 藤枝 直輝, 市川 周一, 命令レジスタファイルを用いた命令の秘匿化, 第 5 回 メニ

ーコア・アーキテクチャ研究会, , 2013, 9, 御殿場
[16] 田村慧, 山田親稔, 市川周一, Coarsely Integrated Operand Scanning アルゴリズムに基づくモンゴメリ乗算器の回路規模縮小手法の検討, 第 12 回情報科学技術フォーラム (FIT 2013), C-016, 2013, 9, 鳥取大学
[17] 松岡俊佑, 市川周一, ハードウェア特殊化 AES 暗号回路のホワイトボックス実装に関する研究, 第 12 回情報科学技術フォーラム (FIT 2013), C-014, 2013, 9, 鳥取大学
[18] 宇山和輝, 市川周一, SSE とアンローリングによる性能向上手法の予備評価, 平成 24 年度電気関係学会東海支部連合大会, A3-2, 2012, 9, 豊橋技術科学大学
[19] 松岡俊佑, 市川周一, ハードウェア特殊化 AES 暗号回路のFPGAへの実装と消費電力の測定, 第 11 回情報科学技術フォーラム(FIT 2012), C-015, 2012, 9, 法政大学
[20] 諸見里斉, 山田親稔, 市川周一, 確定的素数判定法のハードウェア化に関する検討, 電子情報通信学会ソサイエティ大会講演論文集 2011 年_基礎・境界, p.171, 2011, 9, 北海道大学

〔図書〕(計０件)　なし

〔産業財産権〕　なし

〔その他〕
ホームページ等
http://www.ccs.ee.tut.ac.jp/~ichikawa/

６．研究組織
(1)研究代表者

市川　周一 (ICHIKAWA SHUICHI)
豊橋技術科学大学・工学系研究科・教授
研究者番号：70262855

(2)研究分担者

なし

(3)連携研究者

藤枝直輝 (FUJIEDA NAOKI)
豊橋技術科学大学・工学系研究科・助教
研究者番号：　30708425