

平成 29 年度 卒業研究報告書概要

課程, 学籍番号, 氏名	課程: 電気・電子情報工学課程, 学籍番号: B153269, 氏名: 正岡 秀崇
工学分野名: 情報通信システム	指導教員名: 市川 周一, 藤枝 直輝
題 目: 和 MIPS プロセッサに対するパックド IRF 命令の実装と評価 (英 Implementation and Evaluation of Packed IRF Instruction to MIPS Processor)	
Abstract Recently, the defense of software against analysis, plagiarism and falsification has become an important problem. Hines et al. (2005) proposed an Instruction Register File (IRF) and Packed Instructions for power reduction on instruction fetch. Fujieda et al. (2016) used the IRF to protect software. In this study, a Packed IRF Instruction that contains two IRF indices is implemented and evaluated, which extends the design of Fujieda et al. (2016). The target processor is a MIPS32 Release 1 processor distributed on OpenCores and the target FPGA device is Xilinx Artix-7 XC7A35TCPG236-1. According to the evaluation results, the number of logic blocks (slices) was increased by 1.7% and the maximum operating frequency was decrease by 0.1% The reduction of instruction fetch was ranged from 0.05% (dijkstra) to 11.39% (bitcount).	
概 要 近年, 組込みソフトウェアを, 解析・盗用・改ざんから保護する能力, すなわち耐タンパ性の重要性が増加している. 耐タンパ性向上手法の 1 つに, 命令と機械語の対応関係を変更・追加する命令セットランダム化がある. 命令レジスタファイル (Instruction Register File: IRF) は, 使用頻度が高い命令を格納したテーブルである. IRF のインデックスを指定する命令を用い, IRF 内の命令を実行する. Hines ら (2005) は命令フェッチ時の消費電力削減のために, インデックスを 1 つ以上含み, 2 つ以上の命令を 1 つにまとめた命令 Packed Instruction を提案した. 藤枝ら (2016) は, IRF のインデックスを 1 個指定する Specialized Instruction を用いて, IRF を耐タンパ性向上に利用することを提案した. この場合も, IRF のインデックスと命令の対応をシャッフルすることで, 命令セットランダム化がおこなわれる. インデックスを複数持つ命令 (パックド IRF 命令) により電力の削減効果も期待できる. しかし, これまでその定量的な評価はおこなわれていない. 本研究の目的は, パックド IRF 命令を IRF 付き MIPS プロセッサに実装し, ハードウェアリソース消費量と性能に関するオーバーヘッド, および命令フェッチ数を定量的に評価することである. インデックスを 2 つ格納したパックド IRF 命令を, 本研究で定義する. パックド IRF 命令の形式, および付加した IRF 回路は, 藤枝ら (2016) の先行研究を拡張した. 本研究では, nop 命令を示すインデックスを 0 とし, 格納されたインデックス数を判別する. 格納されたインデックスが 1 つならば, 藤枝ら (2016) の Specialized Instruction と同等の処理となる. 本研究では, パックド IRF 命令を OpenCores で公開されている MIPS ソフトコアプロセッサ MIPS32 Release 1 に実装する. MIPS32 Release 1 は 1 クロックに 1 命令ずつ処理する. 本研究では, 分岐命令, 遅延スロットについて, 命令を置換しない場合の評価をおこなった. パックド IRF 命令を実装した MIPS32 Release 1 について, ハードウェアリソース消費量, および最大動作周波数を測定した. シミュレーションより, C 言語版 Dhrystone 2.1, および MiBench (bitcount, dijkstra, stringsearch) における命令フェッチ数も測定した. 実装に用いたデバイスは Xilinx 社の Artix-7 XC7A35TCPG236-1, 合成ツールおよびシミュレータは Vivado 2017.3 である. パックド IRF 命令実装時はベースラインプロセッサよりも, スライス数が 1.7% 増加し, 最大動作周波数は 0.1% 減少した. パックド IRF 命令実装により, 命令フェッチは実装前と比べて 11.39% (bitcount) ~ 0.05% (dijkstra) 減少した. 命令の順序を変更させる場合, および分岐命令と遅延スロットをパックド IRF 命令に置換させる場合の議論を今後の課題とする.	