様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月３１日現在

研究種目：基盤研究(C)
研究期間：２００７～２００８
課題番号：１９５００００３６
研究課題名（和文）　ユビキタスプロセッサ HCgorilla の H/S 協調設計

研究課題名（英文）　H/S co-design of a ubiquitous processor HCgorilla

研究代表者
深瀬　政秋（FUKASE MASA-AKI）
弘前大学・大学院理工学研究科・教授
研究者番号：１０１２５６４３

研究成果の概要：
本研究は、高機能性、柔軟性、信頼性の全てを満たすユビキタスプロセッサとして、マルチコア、マルチパイプの HCgorilla を H/S 協調設計で開拓し、0.18μm CMOS プロセスを用いてチップ化と評価まで実施した。２００７年度は 2.5×5.0mm 角チップで基本構造を実現し、２００８年度はチップ面積を3倍の4.9×7.4mmとしてユビキタスアプリケーションの実行に耐え得る回路規模を確保した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,800,000	540,000	2,340,000
２００８年度	1,700,000	510,000	2,210,000
年度			
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ユビキタスプロセッサ、H/S 協調設計

１．研究開始当初の背景

ユビキタスシステムにまつわるデジタルデバイド、情報洪水、セキュリティ等の懸念を解消すべく提唱されていシステムは総合的な分野を包含するソフト的概念である。このため、その理解と取扱いには高度な IT 知識が引き続き前提となり、ユビキタスの普及に逆行しかねない。IT 格差の解消にはハードウェア面の更なる向上が重要である。プロセッサにはセキュリティと処理効率の向上が必要で、メモリには容量増加が不可欠である。

ハードウェアセキュリティ機能に関して、セキュリティチップは BIOS 改ざんや不正なチップ交換をハード的に禁止するが、RSA 暗号を採用しているため保護対象が短い。

Java チップや携帯用プロセッサのクロック周波数は、ロードマップに明らかなように消費電力抑制の観点から PC プロセッサの数分の１に抑制される。一方、PC プロセッサの技術動向は，処理効率の更なる向上に対処すべく、クロックの高速化からマルチコアに移っている。低電力性と高機能化の相反する課題に対処するため、組み込み系でもマルチコアプロセッサの導入が始まっている。

ユビキタスプラットフォームに搭載するメモリの継続的な増強は、処理スピードとエネルギー消費の削減を妨げている。そこで、高速省電力化等のボトルネックであったファームウェアを必要としないインタープリータ型 Java CPU が有利である。

２．研究の目的

ユビキタスシステムの本質は大小各種の膨大な情報機器群を世界規模で分散し、ネットワーク結合させることにあるので、情報流出が必至の課題である。ユビキタスシステムが真に人間と調和するためには、高機能性、柔軟性、信頼性の全てを満たすことが必要で、そのための基盤技術は SOC である。

ロードマップに見合うプロセスでユビキタスプロセッサの開発研究を行うことを長期的計画として、本研究は我々が開発してきたマルチメディアモバイルプロセッサ gorilla とハードウェア暗号組み込み型プロセッサ RAP を統合し、アプリケーションと開発支援ソフトウェアに配慮して機能付加したユビキタスプロセッサ HCgorilla を開発する。HCgorilla 上で実行させるアプリケーションの言語処理はサーバに負わせ、プラットフォームには必要最低限の実行コードだけを負担させるものとして、命令セットを構築する、並列機構は、マルチコアで双方向高速通信に対応させる。開発対象の HCgorilla は 0.18μm CMOS チップで実践する。

３．研究の方法

２００７年度はマルチコア、マルチパイプの HCgorilla を H/S 協調設計で開拓し、VDEC の 0.18μm CMOS チップで基本構造を実現した。HCgorilla の H/S 協調設計に関して、ソフトウェア側からの実施項目は、ユビキタスの豊富なアプリケーション分析に基づく命令セットの構築、ユビキタスの携帯性と高い普及率を維持するためにマルチコア、マルチパイプに相応しい命令フェッチ機構とソフトウェアの並列機構の調整、並列化コンパイラの設計である。ハードウェア側からの実施項目は以下の通りである。

(1) 命令フェッチ機構の設計：コンパクトな命令フォーマットとストリーム暗号用 SIMD 型命令に対応する可変バイト長命令の自動検出機構と、複数命令を最適パイプラインに自動分配するハードウェア機構を作り上げる。

(2) マルチメディア演算機能の強化：浮動小数点演算回路をメディアパイプに組み込む。

(3) ウェーブ化の最適設計手法の開発：多機能回路のウェーブ化のこれまでの成果をもとに、論理段数とファンアウト間のバランスをとる。更に、設計自由度の乏しいグローバルスタンダードの CAD ツールを離れ，ファインチューニングによるクロックツリーの調整とゲートサイジング手法で、ウェーブ化の最適設計を行う。

(4) チップ試作：設計環境整備（2 台のワークステーションに対する Synopsys と Cadence の CAD ツールとセルライブラリのインストールと整備、東京大学 VDEC と弘前大学間のネットワーク設定）を行い、論理合成，物理設計を行った。これらと平行してウェーブ化を進めた。2.5×5.0mm 角チップで HCgorilla を試作した。

２００８年度はユビキタスアプリケーションの実行に耐え得る回路規模を確保しメモリを増強するため、チップ面積を２００７年度の 2.5×5.0mm 角から 4.9×7.4mm へ 3 倍にして以下を実施した。

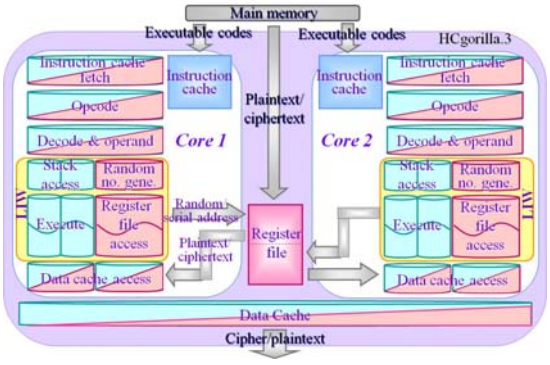
(1) HCgorilla チップの詳細仕様を策定し、チップ面積の増加によって可能となるキャッシュとレジスタファイルの容量を見積った。命令キャッシュの増強に伴う命令フェッチステージの遅延時間増加、レジスタファイルの増強に伴うアクセスステージの遅延時間増加、データキャッシュの増強に伴うアクセスステージの遅延時間増加が予想されるので、論理合成、物理設計に際してそれらの対策を施した。必要に応じて、ウェーブ化の範囲とウェーブ次数を増やし，クロックスピードの最適調整を行い、消費電力の全体調整を行った。

(2)暗号、復号、メディアアプリケーションの各々についてテストプログラムを作成した。３つのテストプログラムの実行コードは、２００７年度に定めた並列化コンパイラの機能に準じてマニアル導出した。

(3) 並列化コンパイラを補完する API と OS の導入を想定し、それらの詳細機能を決めた。

４．研究成果

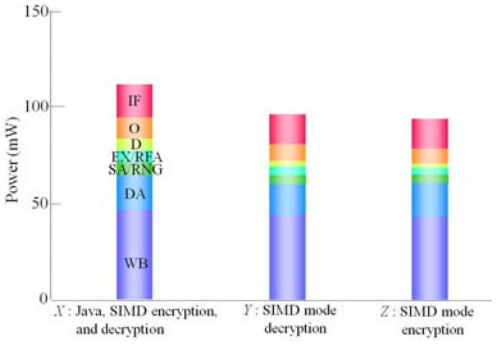
H/S 協調設計で、下図に示すユビキタスプロセッサ HCgorilla を開拓した。



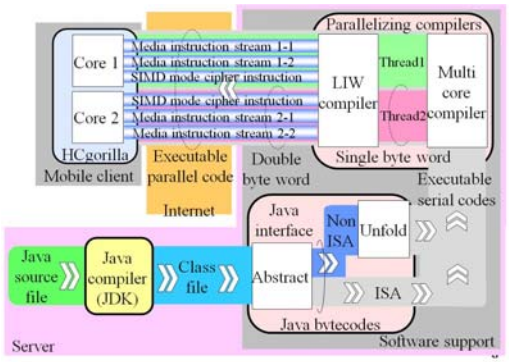
HCgorilla は双方向性通信対応のマルチコア

で、各コアは Java 対応のメディアパイプと独自のハードウェア暗号組み込み型サイファーパイプから成る。

0.18μm CMOS プロセスの 4.9×7.4mm チップでユビキタスアプリケーションの実行に耐え得る回路規模の HCgorilla を試作し、暗号、復号、メディアアプリケーションのテストプログラムで評価した。下図に消費電力の評価を示す。



ソフトウェアに関して、HCgorilla 用アプリケーションの開発支援ソフトをサーバに分離し、ユビキタスプラットフォームの負荷を軽減する下図の方式を構築し、並列化コンパイラと API の詳細機能を決めた。



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１６件）

① Masa-aki Fukase and Tomoaki Sato, “Compilation Techniques Specific for a Hardware Cryptography-Embedded Multimedia Mobile Processor,” Journal of Systemics, Cybernetics and Informatics (印刷中). 査読有

② Masa-aki Fukase, Yusuke Ohsumi, and Tomoaki Sato, “Exploring the Optimum Buffer Size of an Emerging Stream Cipher Engine,” Proc. of ECTI-CON 2009, pp. 607-610, May 2009. 査読有

③ Masa-aki Fukase, Atsuko Yokoyama, and Tomoaki Sato, “A Ubiquitous Processor Embedded with Progressive Cipher Pipelines,” Proc. of GLSVLSI’09, pp. 381-384, May 2009. 査読有

④ Masa-aki Fukase, Kazunori Noda, and Tomoaki Sato, “Emerging Hardware Cryptography and VLSI Implementation,” Proc. of ISPACS, pp. 445-448, Feb. 2009. 査読有

⑤ Masa-aki Fukase, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, “Design and Chip Implementation of the Ubiquitous Processor HCgorilla,” Proc. of ASP-DAC, pp. 129-130, Jan. 2009. 査読有

⑥ Masa-aki Fukase and Tomoaki Sato, “A Ubiquitous Processor Free from Instruction Scheduling,” Proc. of ISCIT, pp. 75-80, Oct. 2008. 査読有

⑦ Masa-aki Fukase and Tomoaki Sato, “Compact FPU Design and Embedding in a Ubiquitous Processor for Multimedia Performance Enhancement,” ECTI-EEC Trans. Vol. 6, No. 2, pp. 79-85, Aug. 2008. 査読有

⑧ Masa-aki Fukase and Tomoaki Sato, “Development of Parallelizing Compilers of a Ubiquitous Processor,” Proc. of WMSCI2008 Vol. II, pp. 220-225, Jul. 2008. 査読有

⑨ Masa-aki Fukase, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, “Enhancing Multimedia Processing by Wave-Pipelining Integer Units and Floating Point Units in Whole,” Proc. of ECTI-CON 2008, IEEE Xplore, pp. II-681-II-684, May 2008. 査読有

⑩ Masa-aki Fukase, Hiroki Takeda, Kazunori Noda, Atsuko Yokoyama, and Tomoaki Sato, “Ad-hoc Cipher by a Ubiquitous Processor,” Proc. of ICESIT, pp. 118-121, Feb. 2008. 査読有

⑪ Masa-aki Fukase and Tomoaki Sato, “A Stream Cipher Engine for Ad-hoc Security,” Proc. of CIS’2007, pp. 902-906, Dec. 2007. 査読有

⑫ Masa-aki Fukase, Kazunori Noda, Hiroki Takeda, and Tomoaki Sato, “Multimedia Performance of a Ubiquitous Processor,” Proc. of ISCIT2007, pp. 1464-1469, Oct. 2007. 査読有

⑬ Masa-aki Fukase, Hiroki Takeda, and Tomoaki Sato, “Hardware/Software Co-Design of a Secure Ubiquitous System,” Computer Intelligence and Security, Springer Berlin/Heidelberg,

LNCS Vol. 4456/2007, pp. 385-395, Sept. 2007. 査読有

⑭ Masa-aki Fukase and Tomoaki Sato, “Exploiting Design and Testing Methods of High-Speed Power Conscious Wave-Pipelines,” Proc. of NASA2007, pp. 5.1.1-5.1.6, June 2007. 査読有

⑮ Masa-aki Fukase, Hiroki Takeda, and Tomoaki Sato, “Hardware Cryptography-Embedded Multimedia Mobile Processor,” Proc. of ECTI-CON 2007, Vol. 2, pp.1128-1131. May 2007. 査読有

⑯ Masa-aki Fukase and Tomoaki Sato, “Design of a Hardware-Cryptography-Embedded Processor for Pervasive Computing,” Proc. of UCAS-3, pp. 15-22, April 2007. 査読有

〔学会発表〕(計１７件)

① 村上亮輔、 横山温子、深瀬政秋、佐藤友暁、「負荷分散型次世代ユビキタスシステム用並列化コンパイラの評価」情報処理学会東北支部研究会、2008 年 12 月 16 日、弘前.査読無

② 大隅裕介、野田一訓、深瀬政秋、佐藤友暁、「Stream cipher engine の性能評価に関する研究」同上、査読無

③ 横山温子、深瀬政秋、佐藤友暁、「ユビキタスプロセッサ HCgorilla 用 Java インターフェースに関する研究」同上.査読無

④ Kazunori Noda, Masa-aki Fukase, and Tomoaki Sato, “Emerging Hardware Cryptography and VLSI Implementation,” 同上、査読無

⑤ 大隅裕介、野田一訓、深瀬政秋、佐藤友暁、「Stream cipher engine の性能評価」平成 20 年度電気関係学会東北支部連合大会, p199. 2008 年 8 月 21 日,郡山.査読無

⑥ 村上亮輔、横山温子、深瀬政秋、佐藤友暁、「負荷分散型次世代ユビキタスシステム用並列化コンパイラ」同上, p224.査読無

⑦ Atsuko Yokoyama, Kazunori Noda, Masa-aki Fukase, and Tomoaki Sato, “A Waved MFU for a Ubiquitous Processor,” 同上, p38.査読無

⑧ Kazunori Noda, Atsuko Yokoyama, Masa-aki Fukase, and Tomoaki Sato, “Exploiting Double Hardware Cryptography,” 同上 p39,査読無

⑨ 野田一訓、横山温子、武田宏樹、深瀬政秋、佐藤友暁、「実行段の多機能ウェーブ化によるマルチメディア機能強化」信学技報, Vol. 107, No. 508 (VLD2007-157, ICD2007-180), pp.7-12, 2008 年 3 月 7 日、那覇.査読無

⑩ 武田宏樹、野田一訓、深瀬政秋、佐藤友暁、「ユビキタスプロセッサ HCgorilla の改良」同上 pp.31-36,査読無

⑪ 武田宏樹、野田一訓、深瀬政秋、佐藤友暁、「HCgorilla の大規模化に関する研究」平成 19 年度電気関係学会東北支部連合大会, p188, 2007 年 8 月 23 日、弘前、査読無

⑫ Kazunori Noda, Hiroki Takeda, Masa-aki Fukase, and Tomoaki Sato, “Multimedia Performance of a Ubiquitous Processor,” 同上, p16 査読無

⑬ 横山温子、武田宏樹、野田一訓、深瀬政秋、佐藤友暁、「HCgorilla のハードウェア/ソフトウェア協調設計に関する研究」同上, p189.査読無

⑭ 岩本祐顕、天間僚、武田宏樹、野田一訓、深瀬政秋、佐藤友暁、「マルチメディアストリーム暗号エンジン」同上, p194.査読無

⑮ 伊藤智恵美、深瀬政秋、佐藤友暁、「ユビキタスプロセッサ HCgorilla 用並列化コンパイラの開発研究」同上、p98.査読無

⑯ 野田一訓、武田宏樹、深瀬政秋、佐藤友暁「HCgorilla のマルチメディア機能強化」情処研報（情報処理学会研究報告）, Vol. 2007, No. 58, (2007-DPS-131), pp. 85-90, 2007 年 6 月 6 日、盛岡.査読無

⑰ Masa-aki Fukase and Tomoaki Sato, “Design Techniques of Wave Pipelines,” IEICE Technical Report, ICD2007-28, pp. 67-72, 2007 年 5 月 31 日、川崎.査読無

〔図書〕(計 １ 件)

① 深瀬政秋、佐藤友暁、「組み込み技術の基礎」津軽地域の産業活性化人材養成事業メカトロニクスシステム要素技術研修テキスト、弘前大学消費生活共同組合, 2008 10 月.

〔産業財産権〕

○出願状況（計 ０件）

○取得状況（計０件）

〔その他〕

① 武田宏樹、野田一訓、横山温子、深瀬政秋、佐藤友暁「ユビキタスプロセッサ HCgorilla の大規模化及び改良」平成 20 年度東京大学大規模集積システム設計教育研究センター年報, p. 181, 2008 8 月. 査読無

② 深瀬政秋, 「ストリームサイファーエンジン」, Embedded Technology2007 公式ガイドブック, p281, 2007 11 月.査読有

③ 深瀬政秋、「Wave pipeline 設計技術」JPCA Show 2007 アカデミック・ラボラトリポスタープログラム講演論文集, pp. 9-14, 2007 5 月.査読有

６．研究組織

(1)研究代表者

深瀬　政秋（FUKASE MASA-AKI）

弘前大学・大学院理工学研究科・教授

研究者番号：１０１２５６４３

(2)研究分担者

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

(3)連携研究者