様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年　4 月 14 日現在

機関番号：１１１０１
研究種目：基盤研究（Ｃ）
研究期間：2009～2011
課題番号：２１５０００４８
研究課題名（和文）　次世代型ユビキタス通信に向けたハードウェア暗号の二重化とＶＬＳＩ実装
研究課題名（英文）　Double cipher hardware scheme for next generation ubiquitous communication and VLSI implementation
研究代表者
深瀬　政秋（FUKASE MASAAKI）
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（和文）：本研究は、RAC (random addressing cryptography)とデータ秘匿を合わせた二重化ハードウェア暗号方式を開発し、VLSI プロセッサに組込み、0.18 μm CMOS の 5.0 mm×7.5 mm チップへ実装した。プロセッサ全体のクロックスピードと消費電力は 200 MHz、275 mW である。Cipher pipe あたりのハードウェアコストは 0.1 mm 角の 270 セルで、スループットは 0.19 GOPS/cipher pipe である。

研究成果の概要（英文）：We have developed, in this study, a double cipher hardware scheme composed of RAC (random addressing cryptography) and hiding data. The cipher scheme has been implemented in a VLSI processor. The clock speed and power consumption of a 0.18-μm CMOS, 5.0 mm×7.5 mm chip are 200 MHz and 275 mW. The throughput and hardware cost of a cipher pipe is 0.19 GOPS and 0.1 mm square filled with 270 cells.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	600,000	180,000	780,000
２０１０年度	1,500,000	450,000	1,950,000
２０１１年度	1,300,000	390,000	1,690,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

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、CMOS、チップ、ハードウェア暗号、二重化暗号

１．研究開始当初の背景

IT 分野の大きな流れであるユビキタス化には、便利さの反面デジタル格差、情報洪水、セキュリティ等の課題も多い。我々はユビキタスネットワーク全体の最適化を目指して、ユビキタスプロセッサ HCgorilla と HCgorilla 用言語処理ソフトの開発、HCgorilla 用ソフトの負荷分散の研究を行ってきた。HCgorilla のチップ化の過程で、RAC のハード的負担は小さくデータ全体を高速暗号化するものの、転字方式であるためデータ自身の秘匿に欠けるという問題が見えてきた。本研究でこれを解決すれば、次世代型ユビキタス通信に相応しいハードウェア暗号技術の開発につながる。

２．研究の目的

本研究では、我々が開発した高速省電力型ハードウェア暗号方式 RAC の暗号強度をデータ秘匿方式で補完する二重化ハードウェア暗号方式を開発する。この方式の有用性を実証するために VLSI プロセッサに組込み、0.18

μm CMOS チップに実装して評価する。

３．研究の方法
データ秘匿回路 HIDU を開発し、マルチコア構造とサイファーパイプを原型とするプロセッサ構造に組み込む。その実用化に向け、小中大 3 つのチップサイズを用いた 3 年計画で実施する。平成 21 年度は HIDU の開発、HIDU と RAC の二重化、二重化ハードウェア暗号機構のストリームファーエンジンへの組み込みを小規模チップで実践する. 平成 22 年度は、チップ規模の拡大に伴うクロックスピード、消費電力、処理能力の劣化をユビキタスのレベルで解消可能なウェーブ化の設計手法を開発し、これを中規模チップで実証する。平成 23 年度は大規模開発で実用化の目処を示す。研究計画の確実性を期すため、チップ化に際しては我々がノウハウを積んでいる 0.18 μm CMOS プロセスを使用する。

４．研究成果
チップ規模の拡大に伴うクロックスピード、消費電力、処理能力の劣化をユビキタスのレベルで解消可能なウェーブ化の設計手法を開発した。具体的な手順は以下の通りである。
マイクロアーキテクチャレベルの調整では、サイファーストリーミングの実用化に見合うべくレジスタファイルとデータキャッシュの容量を増加し、このようなメモリ拡張が引き起こすアクセスステージの遅延時間と電力の増加の対策を施す。必要に応じてウェーブ化の手法を用い、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った。
試作チップの評価項目はクロック、処理時間、命令とデータ処理効率、消費電力などである。評価結果は、プロセッサ全体のクロックスピードと消費電力は 200 MHz、275 mW である。Cipher pipe あたりのハードウェアコストは 0.1 mm 角の 270 セルで、スループットは 0.19 GOPS/cipher pipe である。暗号強度は実用的に十分であるから、二重化ハードウェア暗号は近年重視されている省面積の条件を満たす。

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 17 件）
①Masa-aki Fukase, Kouhei Ichinohe, Naomichi Mimura, Kazuki Narita, Tatsuya Takaki, and Tomoaki Sato, “VLSI Implementation With Double Cipher and Media Processing for Ad-Hoc Network,”, Proc. of ECTI-CON 2012 (In press). 査読有
② Atsushi Kurokawa, Tatsuya Takaki, and Masa-aki Fukase,”Efficient Delay Cells for Wave Pipelined Multifunctional Unit,” Proc. of SASIMI 2012, pp. 121-126, Mar. 2012. 査読有
③Masa-aki Fukase, Harunobu Uchiumi, Kazuki Narita, Tatsuya Takaki, Naomichi Mimura, Kohei Ichinohe, Tomoaki Sato, and Atsushi Kurokawa, “Development of a Next Generation Ubiquitous Processor Chip,” Proc. of ISPACS 2011, pp. 225.1-225.4, Dec. 2011. 査読有
④Masa-aki Fukase, Naomichi Mimura, Kazuki Narita, Tatsuya Takaki, Harunobu Uchiumi, Takumi Ishihara, and Tomoaki Sato, “Evaluation for the Power Conscious Optimum Design of a Ubiquitous Processor,” Proc. of CCCT 2011, Vol. II, pp. 104-108, Jul. 2011. 査読有
⑤Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, Naomichi Mimura, Kazuki Narita, Tatsuya Takaki, and Tomoaki Sato, “Double Cipher Implementation in a Ubiquitous Processor Chip,” Proc. of ECTI-CON 2011, pp.125-128, May 2011. 査読有
⑥Masa-aki Fukase, Takumi Ishihara, Harunobu Uchium, and Tomoaki Sato, “Design and Evaluation of a Waved MFU,” Proc. of APSIPA ASC 2010, p. 70, Dec. 2010. 査読有
⑦Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, and Tomoaki Sato, “Impact of Using a Double Cipher Scheme on the Implementation of a Particular Ubiquitous Processor,” Proc. of ISCIT 2010, pp. 821-826, Oct. 2010. 査読有
⑧Masa-aki Fukase and Tomoaki Sato, “H/S Collaborative Development of a Ubiquitous Processor Free from Instruction Scheduling and Pipeline Disturbance,” Proc. of ICIS 2010, pp. 57-62, Aug. 2010. 査読有
⑨Masa-aki Fukase, AtsukoYokoyama, Takumi Ishihara, Harunobu Uchiumi, and Tomoaki Sato, “Wave Degree versus Dominant Characteristics of a Waved Multifunctional Unit,” Proc. of CCCT 2010, Vol. II, pp. 164-168, Jun. 2010. 査読有
⑩ Masa-aki Fukase and Tomoaki Sato, “A Ubiquitous Processor Built-in a Waved Multifunctional Unit,” ECTI-CIT Trans. Vol. 4, No. 1, pp. 1-7, May 2010. 査読有
⑪ Masa-aki Fukase and Tomoaki Sato, “Exploring the Optimum Buffer Size of an Emerging Stream Cipher Engine,” ECTI-EEC Trans. Vol. 8, No. 1, pp. 53-58, Feb. 2010. 査読有
⑫Masa-aki Fukase, Ryosuke Murakami, and Tomoaki Sato, “Design and Chip Implementation of an Instruction Scheduling Free Ubiquitous Processor,” Proc. of ASP-DAC, pp. 375-376, Jan. 2010. 査読有

⑬ Masa-aki Fukase and Tomoaki Sato, “Performance Evaluation of an Emerging Stream Cipher Engine,” Proc. of APSIPA ASC 2009, pp. 583-588, Oct. 2009. 査読有
⑭Masa-aki Fukase, Harunobu Uchiumi, Takumi Ishihara, Yusuke Osumi, and Tomoaki Sato, “Cipher and Media Possibility of a Ubiquitous Processor,” Proc. of ISCIT 2009, pp. 343-347, Sept. 2009. 査読有
⑮Masa-aki Fukase and Tomoaki Sato, “A Waved Multifunctional Unit on Account of Multimedia Mobile Computing,” Proc. of WMSCI 2009, Vol. III, pp. 86-91, Jul. 2009. 査読有
⑯ 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
⑰ 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

〔学会発表〕（計 34 件）
①内海晴信、深瀬政秋、佐藤友暁「ユビキタスプロセッサチップの独自開発」ETNET2012, 2012 年 3 月 2 日,松島.
②内海晴信、深瀬政秋「次世代型ユビキタスプロセッサチップの開発評価に関する研究」情報処理学会東北支部研究会,弘前,2011 年 9 月 26 日.
③石原拓美、深瀬政秋「ストリームサイファーエンジンのチップ開発に関する研究」情報処理学会東北支部研究会,弘前,2011 年 9 月 26 日.
④成田一貴、内海晴信、石原拓美、三村直道、高木竜哉、深瀬政秋、佐藤友暁「ユビキタスプロセッサの最適設計」FIT2011 函館, 2011 年 9 月 7 日.
⑤内海晴信、石原拓美、三村直道、高木竜哉、成田一貴、深瀬政秋、佐藤友暁「ユビキタスプロセッサチップの開発」FIT2011 函館, 2011 年 9 月 7 日.
⑥ Naomichi Mimura, Harunobu Uchiumi, Takumi Ishihara, Kazuki Narita, Tatsuya Takaki, Masa-aki Fukase, and Tomoaki Sato, “Evaluation of a Double Cipher-Implemented Ubiquitous Processor,” 平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑦高木竜哉、内海晴信、石原拓美、深瀬政秋、黒川敦、佐藤友暁「ウェーブ化 MFU の最適設計」平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑧石原拓美、内海晴信、深瀬政秋、佐藤友暁「ストリームサイファーエンジンのチップ開発評価」平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑨内海晴信、石原拓美、三村直道、高木竜哉、成田一貴、深瀬政秋、佐藤友暁「次世代型ユビキタスプロセッサチップの設計」平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑩野久亮祐、深瀬政秋、佐藤友暁「順序回路のウェーブ化に関する研究」平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑪一戸康平、成田一貴、三村直道、高木竜哉、内海晴信、深瀬政秋、佐藤友暁「Gated clock 実装ユビキタスプロセッサの評価」平成 23 年度電気関係学会東北支部連合大会, 多賀城, 2011 年 8 月 26 日.
⑫内海晴信、石原拓美、深瀬政秋、佐藤友暁「次世代型ユビキタスプロセッサチップの開発」平成 23 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, 2011 年 8 月.
⑬石原拓美、内海晴信、深瀬政秋、佐藤友暁「ストリームサイファーエンジンチップの開発」平成 23 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, 2011 年 8 月.
⑭内海晴信、石原拓美、三村直道、高木竜哉、成田一貴、深瀬政秋、佐藤友暁「ユビキタスプロセッサチップの開発」信学技報, 2011 年 8 月 11 日, 弘前.
⑮深瀬政秋「ユビキタスプロセッサの開発」コラボ産学官第 4 回研究成果発表会、 2011 年 1 月 27 日, 東京.
⑯内海晴信、石原拓美、三村直道、成田一貴、高木竜哉、深瀬政秋、佐藤友暁「ユビキタスプロセッサのチップ開発」信学技報, 2010 年 12 月 16 日, 東京.
⑰内海晴信、石原拓美、三村直道、成田一貴、高木竜哉、深瀬政秋、佐藤友暁「ユビキタスプロセッサのチップ開発」情報処理学会東北支部研究会,弘前,2010 年 12 月 7 日.
⑱ Takumi Ishihara, Harunobu Uchiumi, Masa-aki Fukase, and Tomoaki Sato, “Wave Degree versus Dominant Characteristics of a Waved Multifunctional Unit,” 情報処理学会東北支部研究会,弘前,2010 年 12 月 7 日.
⑲深瀬政秋「負荷分散型ユビキタスネットワーク支援用言語処理ソフトウェアシステムの開発」2008 年度大川情報通信基金研究助成成果概要集, 2010 年 9 月.
⑳大隅裕介、深瀬政秋、佐藤友暁「Stream cipher engine の試作チップ測定」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.
㉑内海晴信、石原拓美、深瀬政秋、佐藤友暁「次世代型ユビキタスプロセッサチップの開発評価」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.

㉒石原拓美、内海晴信、深瀬政秋、佐藤友暁「ストリームサイファーエンジンのチップ開発」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.
㉓三村直道、内海晴信、石原拓美、深瀬政秋、佐藤友暁「ユビキタスプロセッサの評価」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.
㉔成田一貴、蔡京林、石原拓美、内海晴信、深瀬政秋、佐藤友暁「クロックスキーム融合型プロセッサアーキテクチャ」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.
㉕高木竜哉、内海晴信、石原拓美、蔡京林、深瀬政秋、佐藤友暁「ウェーブ化 MFU の基本設計項目の評価」平成 22 年度電気関係学会東北支部連合大会, 八戸, 2010 年 8 月 26 日.
㉖石原拓美、内海晴信、大隅裕介、深瀬政秋、佐藤友暁「ストリームサイファーエンジンのチップ開発」信学技報, 2009 年 12 月 14 日, 静岡.
㉗村上亮輔、横山温子、深瀬政秋、佐藤友暁「ユビキタスプロセッサ用並列化コンパイラの開発」同上, 2009 年 9 月 4 日.
㉘大隅裕介、横山温子、深瀬政秋、佐藤友暁「Stream cipher engine の最適設計」同上, 2009 年 9 月 2 日.
㉙横山温子、大隅裕介、深瀬政秋、佐藤友暁「ウェーブ化 MFU のウェーブ段数依存性」FIT2009, 仙台,2009 年 9 月 2 日.
㉚内海晴信、石原拓美、大隈裕介、深瀬政秋、佐藤友暁「ユビキタスプロセッサの改良」同上, 2009 年 8 月 20 日.
㉛石原拓美、内海晴信、大隅裕介、深瀬政秋、佐藤友暁「Stream Cipher Engine の改良」平成 21 年度電気関係学会東北支部連合大会, 2009 年 8 月 20 日.
㉜石原拓美、内海晴信、大隅裕介、深瀬政秋、佐藤友暁「Stream Cipher Engine Chip の開発」信学技報,2009 年 8 月 11 日,弘前.
㉝野田一訓、深瀬政秋、佐藤友暁「HCgorilla.5 の開発」平成 21 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, 2009 年 8 月
㉞野田一訓、深瀬政秋、佐藤友暁「Stream cipher engine の開発」平成 21 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, 2009 年 8 月

〔その他〕
ホームページ等
http://www.st.hirosaki-u.ac.jp/~shorigaku/index.html

６．研究組織
(1)研究代表者
深瀬　政秋（FUKASE MASAAKI）
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