【29】

氏名	密山幸男（みつやまゆきお）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第 24118 号
学位授与年月日	平成22年6月9日
学位授与の要件	学位規則第4条第2項該当
学位論文名	動画像通信のための信号処理機構のVLSI化に関する研究
論文審査委員	(主査) 教授 尾上 孝雄 (副査) 教授 中前 幸治　教授 村上 孝三 兵庫県立大学特任教授 白川 功

論文内容の要旨

本論文は，動画像通信のための信号処理機能のVLSI化に関する研究について述べたものであり，以下の全6章から構成した．

第1章では，動画像通信処理のための信号処理機構の組込み実装について述べ，本研究の背景と目的を明らかにするとともに，研究内容と成果について概説した．

第2章では，動画像通信システムの概要と，その実装方法について述べた．まず，動画像処理の実装における課題について議論し，その課題を克服すると考えられる再構成可能アーキテクチャの概要について述べた．次に，膨大な動画像データをリアルタイムで暗号・復号処理する共通鍵暗号の実装について述べた．最後に，無線による動画像データ通信の安全性を確保する無線LAN通信向け暗号処理の実装について述べた．

第3章では，メディア処理向け再構成可能アーキテクチャについて述べた．まず，対象アプリケーションをメディア処理に特化することで高い面積効率を実現する粗粒度再構成可能アーキテクチャを提案した．次に，提案するメディア処理向け再構成可能アーキテクチャでの動画像復号処理の実現について述べた．最後に，本再構成可能アーキテクチャのVLSI化を行い，従来アーキテクチャとの比較および，他の実装方式との比較を行った．また，アプリケーション設計における本再構成可能アーキテクチャの拡張性に関する評価を行った．

第4章では，再構成可能アーキテクチャを用いたハードウェア実装向き共通鍵暗号のVLSI化について述べた．まず，再構成可能アーキテクチャの動的再構成機構を暗号アルゴリズムの一部として取り込んだ共通鍵暗号を提案した．次に，そのVLSI化を行い，実装結果について述べた後，他の暗号方式との比較評価を行った．

第5章では，組込みシステム向けIEEE802.11i暗号処理回路のVLSI化とその性能評価について述べた．まず，IEEE802.11iで用いられる共通鍵暗号WEP，TKIP，AES-CCMを対象として，IEEE802.11a/gにおける最大伝送速度での暗号・復号処理を小面積，低消費電力で実現する組込みシステム向けアーキテクチャを提案した．次に，そのVLSI化を行い，実装結果について述べた．

第6章では，本研究で得られた成果を要約し，今後に残された課題について述べ，結論とした．

論文審査の結果の要旨

本論文は、動画像通信のための信号処理機構のVLSI化に関する研究の成果をまとめたものであり、以下の主要な結果を得ている。

(1) メディア処理向け再構成可能アーキテクチャのVLSI化

多様な動画像通信アプリケーションを実現する携帯情報端末において、ハードウェア資源の厳しい制約を満たしながら、複数の動画像符号/復号アルゴリズムに対応できる柔軟性が求められている。本論文では、対象アプリケーション分野をメディア処理に特化することで，複数の動画像処理方式に対応しながら高い性能面積効率を実現する再構成可能アーキテクチャを提案している。提案アーキテクチャのVLSI化設計を行った結果、従来アーキテクチャと比較して約3.5倍の性能面積効率を実現している。さらに、再構成可能セルアレイのスケーラビリティと，動画像復号処理の画素並列性を活かすことで、高性能化要求に対する性能拡張が可能であることを示している。

(2) 再構成可能アーキテクチャを用いたハードウェア実装向き共通鍵暗号のVLSI化

情報通信環境を活用したアプリケーションの多機能化にともない、情報の秘匿や著作権保護のための技術として、通信データの暗号化が不可欠となっている。本論文では、膨大な動画像データを実時間で暗号・復号処理するハードウェア実装向き共通鍵暗号を提案している。提案共通鍵暗号は、暗号処理との親和性の高いマルチコンテクスト型動的再構成可能アーキテクチャを暗号アルゴリズムの一部に採用しており、従来の暗号方式と比較して、ソフトウェアによる解読試行に対して12.3倍の耐性を有しながら、ハードウェア実装による高い処理性能を実現している。また、再構成可能アーキテクチャの構成情報を暗号鍵の一部と見なすことにより、セキュリティ要求に応じて柔軟な構成情報の取り扱いを可能としている。

(3) 組込みシステム向けIEEE802.11i暗号処理回路のVLSI化

無線LANセキュリティ拡張規格IEEE802.11iで用いられる暗号処理には膨大な演算量が必要であり、組込みプロセッサによるソフトウェア実装では十分な処理速度の達成が困難である。本論文では、IEEE802.11iで用いられる共通鍵暗号WEP、TKIP、AES-CCMの組込みシステム向けアーキテクチャを提案している。WEP/TKIPにおけるシャッフリング処理では、2個のデータを結合したメモリアクセスによりメモリアクセス回数の削減している。また、AES-CCMでは、2種類のAES処理のパイプライン化により小面積化と高性能化を実現している。提案処理回路のVLSI化設計を行った結果、18,000ゲートの回路規模と15mWの消費電力で、60MHz動作時にIEEE802.11a/g規格の最大伝送速度での暗号・復号処理を可能としている。

以上のように、本論文で述べた動画像通信のための信号処理機構のVLSI化に関する研究は、限られたハードウェア資源で必要な処理性能を実現する信号処理機構の実装方針を示したという点で非常に有用である。これにより、携帯情報端末においても多様な動画像通信アプリケーションの提供が可能となり、動画像通信システムの普及と発展に貢献するものと期待できる。よって、博士（情報科学）の学位論文として価値あるものと認める。