平成20年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	安 藤　友 樹
卒業研究題目	システムレベル設計環境SystemBuilderを用いたAES暗号化システムの設計事例	

近年，組込みシステム開発では，システムレベル設計が注目を集めている．従来の組込みシステム設計では，仕様段階で，設計者の経験と勘に基づきソフトウェア/ハードウェア分割が決められていた．その後，ソフトウェアとハードウェアの詳細設計が別々になされるため，設計終了後にはじめて，仕様ミスが発覚することがあった．一方，システムレベル設計では，まず，システム全体の仕様を高い抽象度で記述した後，ソフトウェア/ハードウェア分割などの設計探索を行い，ハードウェア面積とシステムの処理時間のトレードオフを取得する．設計探索で得たトレードオフをもとに，ソフトウェアとハードウェアの詳細な仕様を決定できるため，設計終了後の仕様ミス発覚が軽減される．設計者が短期間でソフトウェア/ハードウェア分割のトレードオフを得るために，高い抽象度で記述されたシステムの機能や通信から，シミュレーション記述や，実装レベルの記述を自動合成するシステムレベル設計ツールが，研究開発されている．

私が所属する研究室では，システムレベル設計環境であるSystemBuilderを開発した．SystemBuilderは，C言語で記述されたシステム機能と，ターゲットアーキテクチャへのマッピング情報を入力とし，FPGA上の実装を自動合成する．SystemBuilderは機能のマッピング情報をもとに，自動で機能間の通信を合成する．SystemBuilderを用いることで，設計者が通信設計をする必要がなくなり，ソフトウェア/ハードウェア分割，システムのパイプライン構造化といった，アーキテクチャの設計探索が容易となる．

本論文ではシステムレベル設計の設計探索に関する2つの研究について述べる．まず「システムレベル設計環境SystemBuilderを用いたAES暗号化システムの設計事例」を示す．続いて,「複数アプリケーションによるハードウェア共有」について述べる．

SystemBuilderの設計効率を評価することを目的として，AES暗号化システムを設計した．設計目標を，ハードウェアパイプライン実装によるシステムの実行時間短縮と設定した．さらに，設計効率を評価するために設計期間を記録した．ソフトウェアプログラムとして実装されたAES暗号化システムを設計の起点とした．システム構成を徐々に変更しながら，ソフトウェアのみで実装されたシステムより，実行時間が80 %削減されたハードウェアパイプライン実装のシステムを設計できた．ハードウェア設計の経験がない設計者が，1週間強という短期間でハードウェアパイプライン実装のシステムを設計したことより，SystemBuilderの高い設計効率が確かめられた．

ハードウェア面積の削減を目的とした探索のため，複数アプリケーションによるハードウェア共有の合成方法を提案した．アプリケーションでは，性能を向上するために処理の一部を，専用ハードウェアとして実装することがある．しかし，多くのアプリケーションの処理をハードウェアとして実装すると，ハードウェア面積の制約を満たさないことがある．この際，複数のアプリケーションで同じ処理を共有し，ハードウェアの面積を削減できる．システムレベル設計では，共有を意識していない記述から，共有可能なハードウェアを合成できることが望ましい．本研究では，システムの通信が高い抽象度で記述されていることを前提とし，システムの機能記述に変更を加えず，通信の自動合成のみにより，ハードウェアの共有を可能とする通信方式を提案した．AES暗号化システムを2つ用意し，提案通信方式を適用した．実験により，システムがハードウェアを共有し，正常に動作することを確認した．ハードウェアで実装された処理を共有することで，面積が最大で37 %削減された．提案通信方式により，ハードウェア共有が可能であることが確認できた．