Cプロトタイプ解析によるハード／ソフト最適分割システムの構築とマルチコアへの適用

和田智行†　山崎勝弘†
立命館大学大学院　理工学研究科†

1. はじめに

本研究では、ハードウェアとソフトウェアの最適な分割を実現するために、対象となる問題の C 言語のソフトウェアプロトタイプが完成した段階で、プロトタイプを解析して、ハードウェアとソフトウェアの最適な分割点を見つけ出すシステムの構築を目的とする[1]。また、このシステムをマルチコア環境にも適用することを目指す。本稿では、本システムの解析手法と Misty1 暗号への適用結果を示し、本システムの有効性を検討する。

2. ハード／ソフト最適分割システム

2.1 システム構成

ハードウェアとソフトウェアを最適に分割する手法には現状では設計者による経験則からの試行が多い。それに対し、本研究では C 言語により記述されたプロトタイプを解析して、機械的かつ早期に分割案を提示することにより、設計者を支援することを目指す。ハード／ソフト最適分割システムの構成を図 1に示す。

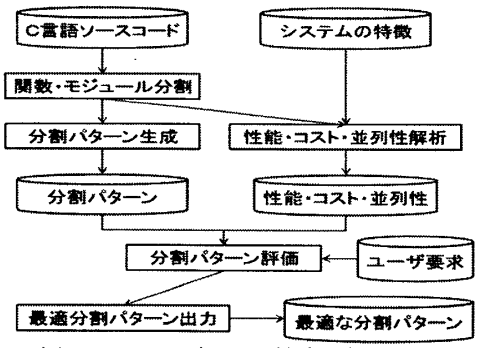

図 1：ハード／ソフト最適分割システム

本システムの入力は完成したハードウェアのリファレンスとなる C ソースコード、実験対象の環境などのシステムの特徴を数値化したもの、及びユーザ要求を数値化したものである。システムの特徴は、主に実験対象のプロセッサの命令セットやアーキテクチャから予め抜き出したもので、命令毎のクロック数、パイプライン段数などである。ユーザ要求は処理速度、回路規模、並列性などの解析項目に対して重みを付加したものと各性能に対する足きり項目である。まず、C ソースコードとシステムの特徴より、性能・コスト・並列性の解析をそれぞれ行う。また、C ソースコードより全分割パターンを生成し、解析結果とユーザ要求を合わせることで評価を行い、優れたパターン候補を出力する。

Best Partitioning System of Hardware and Software with C prototype Anlysis and Applying to Multi-Core, Tomoyuki Wada and Katsuhiro Yamazaki, Graduate school of Science and Engineering, Ritsumeikan University

2.2 解析手法

ハード／ソフト最適分割システムの UML による仕様を図 2に示す。本システムでは関数・モジュール毎に解析を行う。まず、前処理部で関数・モジュール部分の抽出を行う。またこのとき、変数、プリプロセッサ、FSM など、解析に必要となるものも構造解析し、抜き出す。前処理部より抜き出した情報を元に、性能・コスト解析部、並列性解析部で解析を行う。性能・コスト解析部では、SW／HW クロック数、回路規模、メモリ使用量、データパス、及び各モジュールの負荷割合を算出する。並列性解析では、データ並列、パイプライン並列が可能であるかを解析し、適切な並列数も解析する。これらの解析結果を生成した全分割パターンで評価することで、最適な分割パターンの出力を行う。

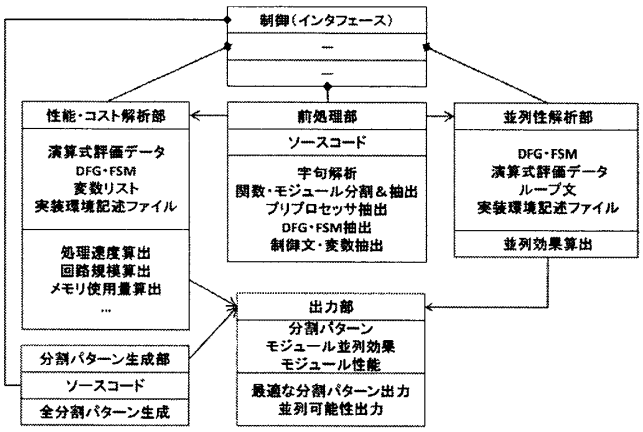

図 2：ハード／ソフト最適分割システムの UML による仕様

3. Misty1 に対するハード／ソフト最適分割

3.1 Misty1 暗号アルゴリズム

Misty1 は 128 bit 秘密鍵／64bit ブロック暗号である。データを分割して排他的論理和やテーブル参照を行うことを変換処理の基本にしている。条件分岐などは一切存在しない、非常にハードウェア化を意識したアルゴリズムとなっている。ループ回数は 4 の倍数であれば良いが、推奨ループ数は 8 とされている。図 3に Misty1 暗号の処理フローを示す。Misty1 の関数・モジュールは主に FO・FI・FL・KeyScheduling（KS）の 4 つからなる。関数が入れ子になっており、図中の FO 関数は更に FI 関数を包含している。また、図中の S9・S7 はテーブル参照を行う関数である。KS は拡張鍵生成モジュールであり、FL 関数を 8 つ包含している。使用する鍵は秘密鍵・拡張鍵を分割しループ数毎に合った鍵を渡す。

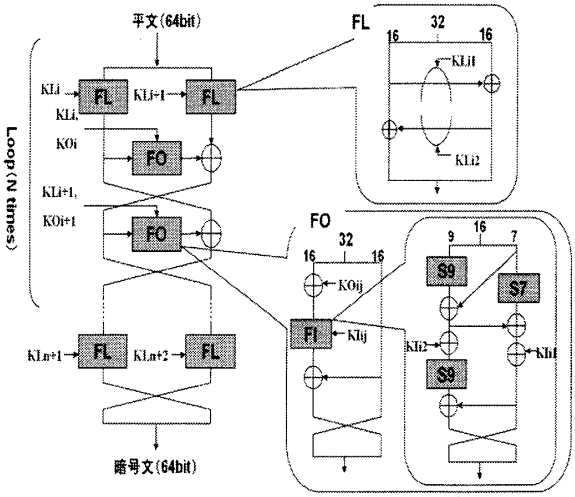

図 3：Misty1 暗号の基本構成

3.2 ハード／ソフト最適分割システムの適用

ハード／ソフト最適分割システムでは、速度・回路規模・バランス・ユーザ要求の 4 つの項目を重視した分割パターンを出力する。各パターンで各モジュールがハードウェアとソフトウェアのどちらで実装するのがよいか出力する。また、設計者への参考情報として各モジュールの性能・コストも出力する。Misty1 を FL・FO・FI・KS の 4 つの関数に分割し、ループ回数を 8 とし、ハード／ソフト最適分割システムに適用した。実装ターゲットのプロセッサと FPGA は Xilinx 社の"MicroBlaze"と"Vertex4 LX60"である。表 1・表 2に Misty1 暗号システムにおけるハード／ソフト最適分割システムの出力結果を示す。 表 1は重視項目毎の分割パターンとその回路規模と実行サイクル数を示す。表 2は各モジュールの性能・コストを示す。表 1の各分割パターンにおける H はハードウェア、S はソフトウェアを示す。ただし、ハード／ソフト最適分割システムは試作中であるため、一部は手計算による計算結果である。

表 1：Misty1 暗号システムの分割案

	FI	FO	FL	KS	回路規模[Slices]	実行サイクル数[Cycle]
速度	H	H	H	H	3696	1442
回路規模	S	S	S	S	0	4420
バランス	H	H	H	S	800	1972

表 2:Misty1 暗号の各モジュールの性能

	FI	FO	FL	KS
回路規模[slices]	256	784	16	2064
メモリ量[Bytes]	28	140	24	232
SW 実行サイクル数[clocks]	47	247	48	576
HW 実行サイクル数[clocks]	1	4	1	12
SW 負荷割合[%]	45	47	10	12
最高動作周波数[MHz]	88	20	108	35

3.3 システム評価

3.2 節で出力された分割パターンを実装・実測し評価することでハード／ソフト最適分割システムによる解析結果の整合性と分割案の妥当性を評価する。表 3に Misty1 暗号システム分割案の実測結果を示す。

表 1の解析結果と表 3の実測結果を比較すると、性能・コストの解析結果の整合性は高いといえる。表 2における性能の解析結果の誤差は実測値を 1 とすると平均 0.2 の誤差であり、概ね妥当な整合性を持っているといえる。パターン毎の評価として、速度・回路規模重視はそれぞれハードウェアかソフトウェアのみのパターンとなり妥当であるといえる。これらは、入力時に最高動作周波数やメモリ量に対して足きり値を与えることで結果が変わる。バランス重視はモジュールのハードウェア化の効果が高いものが選出されている。使用頻度が低い KS をハードウェア化せず、使用頻度が高く、負荷の大きい FO・FI・FL をハードウェア化することが望ましいと判断していることから妥当であると考えられる。

表 3：Misty1 暗号システム分割の実測結果

	回路規模[Slices]	実行サイクル数[Cycles]
速度	3436	1467
回路規模	0	3918
バランス	1093	1782

4. マルチコアへの適用

本システムではマルチコア環境を考慮したハード／ソフト分割における解析も行う。各モジュールに対してマルチコア環境を考慮した場合の並列可能性と最適な並列度の算出を行い評価する。

本システムの検証には Xilinx 社のソフトマコアプロセッサ"MicroBlaze"を中心として使用する。図 4に本研究で使用する検証システムの構成を示す。MicroBlaze プロセッサに BlockRAM を接続し、これに命令データを格納する。システムのハードウェア処理となるモジュールや評価用のクロックカウンタは FSL（Fast Simplex Link）というバスを通して接続しており、2 クロックサイクル以内でデータ転送が可能である。このシステムに複数の自作プロセッサを接続することでマルチコア環境の構築も行う。動作結果の確認は PC と通信することで行う。OPB(On-Chip Peripheral Bus)を通して、シリアル通信用の IP である UART を接続することで可能となる。自作ハードウェアにプロセッサを接続することでマルチコア環境を構築し検証することが可能である。

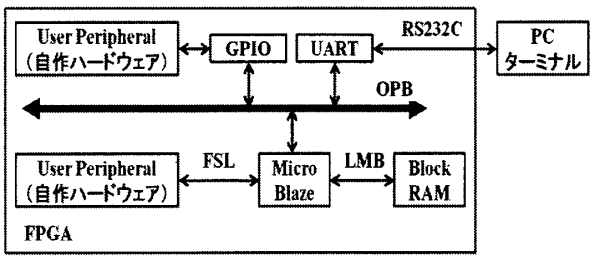

図 4：MicroBlaze 検証システム

5. おわりに

本稿ではハード／ソフト協調設計におけるハードウェアとソフトウェアの最適な分割を行うシステムを提案し、その構成や処理内容などについて述べた。また、暗号アルゴリズムである Misty1 を対象として、本システムを適用し、システムの検証を行った。さらに、マルチコア環境におけるシステムの適用を検討した。

参考文献

[1] 梅原直人：設計仕様解析によるハード／ソフト最適分割システムの構築と評価，FIT2007，C-001，2007.