MD5計算回路Panchamの移植と改良

指導教官 市川周一　　学籍番号 013744　丸山裕

1　はじめに

MD5 [1] は，任意の長さのメッセージから 128 ビットのメッセージダイジェストを生成する関数である．MD5 は，チェックサムや IPsec [2] に応用することができる．MD5 計算回路 Pancham [3] は，MD5 を計算する GPL の IP コアである．Pancham は Verilog で書かれており，論理合成することで任意のハードウエアに実装することができる．本研究では，Pancham を Verilog から VHDL に移植し，さらに性能改良を行った．移植後の回路は，オリジナルと同じく GPL として公開予定である．

2　移植作業と改良

VerilogHDL から VHDL へ移植し，改良を行った．移植前と移植後のソースのサイズを表 1 に示す．

表 1: ソースのサイズ

Verilog	[行]	[KB]	VHDL	[行]	[KB]
pancham.v	505	15.9	md5.vhd	783	23.1
pancham_round.v	154	3.6	round.vhd	55	1.3
pancham.h	99	2.8	my_shift.vhd	163	3.3
			padding.vhd	539	16.4
合計	758	22.3	合計	1540	44.2

設計環境を以下に示す．ホスト PC は AthlonXP 2400+, Memory 1 GB, WindowsXP Professional　SP1 である．使用したツールを表 2 に示す．

表 2: ターゲットデバイスと CAD ツール

ターゲットデバイス	CAD ツール
Altera Stratix	QuartusII 3.0
Xilinx Virtex-II	Synopsys FPGA CompilerII 3.7 Xilinx ISE 5.2i

VHDL に直したあと，以下のような設計改良を試みた．

1. シフタの改良

   SHIFT1 シフタの冗長部分を削除する．

   SHIFT2 固定長シフタを切り替える設計に変更する．

2. 加算器の改良

   ADD1 Process 文から加算器を外す．

   ADD2 コンポーネントを分離する．

3. Altera のパラメタライズドモジュールライブラリ LPM[4] を使う．

   LPMADD LPM_ADD を使う．

   LPMSHIFT LPM_CLSHIFT を使う．

3　評価

改良した設計を，Altera Stratix FPGA 用と，Xilinx Virtex-II FPGA 用に実装設計した結果を，それぞれ表 3 と表 4 に示す．AT 積は，論理規模と実行時間の積である．

表 3: ターゲットデバイス EP1S10F780C7ES

ソース	規模 [LE]	動作周波数 [MHz]	AT 積 [LE·μs]	スループット [Mbps]
Verilog	4148	37.00	7399	287
VHDL	3083	38.61	5815	288
SHIFT1	2991	36.93	5345	286
SHIFT2	2743	41.12	4403	324
ADD1	2784	41.77	4399	300
ADD2	2784	41.77	4399	324
LPMADD	2787	42.11	4368	327
LPMSHIFT	2889	35.82	5323	278

表 4: ターゲットデバイス XC2V3000G676

ソース	規模 [Slice]	動作周波数 [MHz]	AT 積 [Slice·μs]	スループット [Mbps]
Verilog	6698	50.18	8809	389
VHDL	1858	70.82	1731	549
SHIFT1	2179	51.62	2786	400
SHIFT2	1987	65.06	2016	504
ADD1	1748	58.81	1962	456
ADD2	1756	70.51	1644	547

Diez ら [5] は，Virtex-II XC2V3000 を用いた MD5 回路の性能を報告している（表 5）．本研究で作った Virtex-II 2V3000 を用いた回路のうち，最も AT 積の小さい ADD2 と比べると，論理規模は 1.3 倍であるが，動作速度は 1.2 倍である．AT 積は 1.1 倍程度増えている．

表 5: Diez ら [5] の回路

規模 [Slice]	動作周波数 [MHz]	AT 積 [LE·μs]	スループット [Mbps]
1369	60.20	1501	467

性能比較のため，RFC1321 サンプル実装を gcc 2.95.3 でコンパイルし，ソフトウェアの実行速度を計測した．測定環境は，AthlonXP 2600+，メモリ：1 GB，OS：VineLinux 2.6 r1，コンパイルオプションは -O である．計測した結果，ソフトウェアのスループットは 1198.3 Mbps であった．設計した回路のうち，最も高速なもの（Virtex-II の VHDL 記述，スループット 549.4 Mbps）と比較すると，2.1 GHz 動作のプロセッサに対し，70 MHz 動作の専用回路で約 0.46 倍の動作速度を発揮する．

4　おわりに

MD5 計算回路 Pancham を VerilogHDL から VHDL へ移植し，Altera Stratix 用に最適化した．この VHDL 記述は，Xilinx Virtex-II 用にも実装設計できることを確認した．Stratix で最適化した設計を Virtex-II 用に実装設計しても最適な結果は得られなかったが，最適化なしの VHDL 記述でも元の VerilogHDL 記述より論理規模が小さくスループットが高くなることがわかった．

移植した VHDL 記述は，まだ実 FPGA チップ上で動作確認を済ませていない．早急に実機で動作を確認して，この VHDL 記述を GPL で公開したい．

参考文献

[1] Rivest, R. L. : RFC 1321 – The MD5 Message-Digest Algorithm，http://www.faqs.org/rfcs/rfc1321.html.

[2] Kent, S. : RFC 2401 - Security Architecture for the Internet Protocol，http://www.faqs.org/rfcs/rfc2401.html.

[3] Mittra, S. : Pancham An MD5 compliant IP core, http://pancham.sourceforge.net/.

[4] Library of Parameterized Modules (LPM), http://www.altera.co.jp/products/software/pld/products/maxplus2/sfw-lpm.html.

[5] Diez, J. M., Bojanic, S., Stanimirovic, Lj., Carreras, C., Nieto-Taladriz, O.: Hash Algorithms For Cryptographic Protocols: FPGA Implementations, TELFOR'2002, Belgrade, Yugoslavia, Nov. 26–28, 2002.