

動的部分再構成による回路規模と消費電力の削減についての一考察

堀 洋平[†] 坂根 広史[†] 戸田 賢二[†]

[†] 独立行政法人 産業技術総合研究所 〒305-8568 茨城県つくば市梅園 1-1-1 中央第2 事業所
E-mail: †{hori.y,hirofumi.sakane,k-toda}@aist.go.jp

あらまし FPGA の動的部分再構成を利用し、複数のモジュールを切り替えて実装することで、回路面積や消費電力がどの程度削減可能であるか評価した。現在市販されている FPGA には、回路の一部のみを動作中に再構成可能なものがあり、様々な機能を環境や用途に合わせて柔軟に変更するとともに、回路規模や消費電力の削減につながると期待されている。今回、6つの標準的な暗号モジュール (AES, Camellia, SEED, TDEA, MISTY1, CAST-128) を使い、これらを同時に実装した場合と、1つずつ切り替えて実装した場合のリソース使用量と消費電力を評価した。
キーワード FPGA, リコンフィギャラブル・コンピューティング, 動的部分再構成, 回路規模, 消費電力

A Study of the Effectiveness of Dynamic Partial Reconfiguration for Size and Power Reduction

Yohei HORI[†], Hirofumi SAKANE[†], and Kenji TODA[†]

[†] National Institute of Advanced Industrial Science and Technology
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba-shi, Ibaraki 305-8568, Japan
E-mail: †{hori.y,hirofumi.sakane,k-toda}@aist.go.jp

Abstract We evaluated the effectiveness of the partial reconfiguration in reducing area and power consumption of an FPGA-based circuit. We implemented 6 cryptographic modules (AES, Camellia, SEED, TDEA, MISTY1, CAST-128) on the partially reconfigurable and non-reconfigurable circuits. According to the experimental results, the area efficiency is considerably improved by using the partial reconfiguration. The results also shows that the power consumption is slightly improved in the most cases, but that there could be an exceptional case.

Key words FPGA, reconfigurable computing, run-time partial reconfiguration, area efficiency, power consumption

1 はじめに

回路構成を変更可能な論理デバイスである Field-Programmable Gate Array (FPGA) は、プロセス技術の進歩とともに集積度・回路規模が向上し、近年では開発用途だけでなく幅広い民生機器等に搭載されるようになった。現在市販されている一部の FPGA は、他の部分の演算を停止させることなく回路の特定部分のみを書き換える動的部分再構成 (Dynamic Partial Reconfiguration: DPR) の機能を備えている。DPR を利用することで、環境や用途に合わせて回路の機能を変更する柔軟なシステムが実現できると期待されている。また、同一の領域において複数のモジュールを切り替えて使用することができるため、実装面積や消費電力が削減されると期待されている。

今回、ISO/IEC 18033 [1] にブロック暗号の標準として採用された 6つの共通鍵暗号アルゴリズム (AES, Camellia, SEED, TDEA, MISTY1, CAST-128) を、部分再構成を利用した場合と

しない場合において実装し、回路規模や消費電力がどの程度削減できるかを評価した。本稿において、実装された回路の構成と、面積・消費電力の削減効果について述べる。

2 ザイリンクス FPGA における動的部分再構成

2.1 Early Access PR

DPR 回路の設計手順を解説したものとして、アプリケーションノート XAPP290 [2] や開発システムリファレンスガイド [3] があるが、現在ではこれらの手順に従うことは推奨されない。現在の DPR 回路の設計手順は Early Access Partial Reconfiguration (EA PR) design flow と呼ばれており、旧来手順における制約が緩和され、設計が飛躍的に容易になった。EA PR の手順については文献 [4] にも述べられているが、この手順は 2007 年 8 月にさらに改良されたため、最新のドキュメント [5] を参照することが望ましい。

EA PR に関するドキュメントやリファレンスデザイン等のリ

ソースは、ザイリンクスのウェブサイト上にある EA PR Lounge から入手可能であるが、このサイトへアクセスするにはユーザ登録をする必要がある。EA PR Lounge やユーザ登録申請ページの URL を公開することは禁止されており、アクセスを希望するユーザはザイリンクスの技術サポートに問い合わせなければならない(学生は指導教官の許可が必要)。

2.2 開発ツール

ER PR では、ザイリンクスの統合開発環境 ISE に、特殊なパッチを当てたものを使用する。このパッチは、前節で述べた EA PR Lounge から入手可能である。現時点で最新のものは、ISE9.1i+sp2 用のパッチである。また、DPR 回路の設計には通常の ISE には含まれないツール群が必要であるが、これらはパッチの適用時にインストールされる。

ザイリンクスのデザイン解析ツール PlanAhead [5] を使用すると、DPR 回路に特有の制約が簡単に設定できるため、設計が飛躍的に容易になる。PlanAhead は、フロアプラン、配置配線、タイミング解析、およびモジュールベースのインクリメンタルな設計等を行うためのツールであるが、DPR 回路の開発プラットフォームとして利用することが可能である [6]。ただし、初期状態の PlanAhead は DPR 回路開発の支援機能が無効になっており、これを有効にするための Tcl コマンドに関する情報を EA PR Lounge から入手する必要がある。

2.3 DPR 対応デバイス

現在市販されている FPGA の中で部分再構成が可能なものは、ザイリンクスの Spartan シリーズと Virtex シリーズである。この中で、動的な部分再構成ができるのは Virtex シリーズである。Spartan シリーズはコンフィギュレーションがグリッチレスに行われなため、再構成中の固定回路の動作を保証することができず、動的な部分再構成を行うことは推奨されない。また、Virtex-II 以降の Virtex シリーズでは、自己再構成が可能である。

リファレンスデザイン [3] の記述では、様々な Virtex シリーズや Spartan シリーズにおいて旧設計手順が適用可能とされていたが、最新の情報^(注1)では適用不可(もしくは非推奨)とされている。ザイリンクス FPGA の部分再構成対応状況について、表 1 にまとめる。表 1 は 2007 年 12 月時点の対応状況であり、今後変更される可能性がある。

2.4 部分再構成モジュール

EA PR 回路では、通常は長方形のモジュール単位で部分再構成を行う。このとき、部分再構成の対象となるモジュールを **Partially Reconfigurable Module (PRM)** と呼び、そのモジュールが配置されるデバイス上の領域を **Partially Reconfigurable Region (PRR)** と呼ぶ。長方形領域以外に、複数の長方形をつなぎ合わせた多角形領域を PRR に設定することも可能とされている。Virtex-II Pro 以前のデバイスでは、PRR は任意の大きさの長方形とすることができるが、部分再構成フレームはカラム単位である。(図 1 左)。Virtex-4/5 では、PRR は任意の大きさの長方形であり、部分再構成フレームの上下の境界はクロッククリージョンの境界に等しい(図 1 右)。

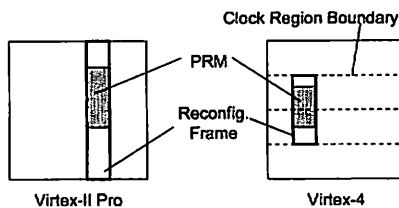


図 1 部分再構成フレーム

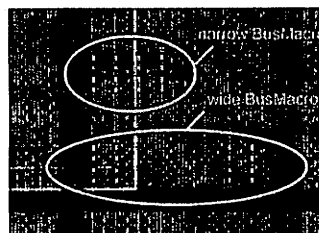


図 2 スライスベース・バスマクロ

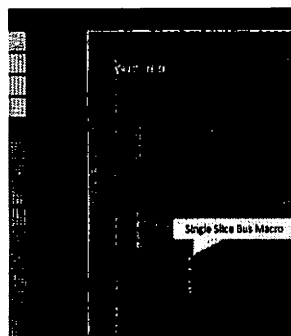


図 3 シングルスライス・バスマクロ

2.5 バスマクロ

DPR では、部分再構成後の配線が正しく結線されることを保証する必要がある。ザイリンクス FPGA では、バスマクロと呼ばれるハードマクロを用いてこれを実現する。PRM と固定モジュール、あるいは 2 つの PRM の間の信号は、必ずバスマクロを通らなければならない(クロック等のグローバル信号を除く)。バスマクロの位置を常に一定にすることで、部分再構成後の信号が確実に結線される。

Virtex-4 までのデバイスでは、スライスベース・バスマクロを使用する。スライスベース・バスマクロは、縦 4 個、横 4 個の合計 16 個の Look-up Table (LUT) から構成される配線済みハードマクロである。スライスベース・バスマクロは、左から右、あるいは右から左のどちらか一方に 8 bit 幅の信号を通過させる。また Virtex-4 に限り、上から下、および下から上方向のバスマクロも存在する。さらに、信号の向きの違いのほか、同期/非同期、イネーブル付き/イネーブルなし、narrow/wide の区別がある。Narrow バスマクロの横幅は 2 CLB、wide は 4 CLB である(図 2)。Wide バスマクロを 3 つ並べて使用することにより、縦幅 2 CLB の境界において最大 24 bit 幅の信号を通過させることが可能となる。

(注1): E-mail による Xilinx との私信, 2006 年 12 月 13-15 日。

表1 ザイリンクスデバイスの部分再構成対応状況

Device	Old XAPP290 flow	EA PR flow	Glitchless	PlanAhead support
Virtex	○	○ (untested)	○ (untested)	×
Virtex-E	○	○ (untested)	○ (untested)	×
Virtex-II	○ (untested)	○	○	All*
Virtex-II Pro/-II ProX	×	○	○	All*
Virtex-4	×	○	○	All*
Virtex-5	×	○	○	All*
Spartan	×	○ (untested)**	×	×
Spartan-II/-III	×	○**	×	×
Spartan-3/-3L/-3E	×	○	×	floorplan, constrain, export
Spartan-3A	×	○	×	floorplan, constrain, export

* All = floorplan, constrain, export, map, PAR, assemble.

** 現時点ではバスマクロが提供されていない。

Virtex-5におけるバスマクロはシングルスライス・バスマクロと呼ばれ、4個のLUTから構成される。シングルスライス・バスマクロは、モジュール境界をまたぐ従来の配置方法ではなく、PRR内部の任意の場所に置く(図3)。また従来バスマクロと異なり、信号の向きを考慮する必要はない。シングルスライス・バスマクロは、今後Virtex-4においてもサポートされるとされている。

2.6 Internal Configuration Access Port

Virtex-II以降のVirtexシリーズFPGAには、内部ロジックからコンフィギュレーションメモリにアクセスするためのInternal Configuration Access Port (ICAP)と呼ばれるプリミティブがある。ICAPを通じて、コンフィギュレーションメモリを読み書きすることが可能である。自己再構成を行う際は、ICAPが必須となる。

3 共通鍵ブロック暗号

今回、ISO/IEC 18033-3で標準として採用された6つのブロック暗号アルゴリズムを実装した。ISO/IEC 18033-3では、128 bit ブロック暗号としてAES, Camellia, SEED, また64 bit ブロック暗号としてTDEA, MISTY1, CAST-128が採用された。本章では、これらのアルゴリズムについて簡単に説明する。

3.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) [7]は、危殆化が懸念されるData Encryption Standard (DES) [8]に変わる新しい暗号規格として、National Institute of Standard and Technologies (NIST, 米国国立標準技術研究所)によってFIPS 197として公表された。AESはSubstitution-Permutation Network (SPN) 構造のブロック暗号で、ブロック長は128 bit、鍵長は128, 192, 256 bitのいずれかを選択できる。ラウンド数は、128, 192, 256 bitの鍵に対してそれぞれ10, 12, 14段となる。米国の標準暗号規格であり、欧州のNew European Schemes for Signature, Integrity, and Encryption (NESSIE)で採用されているほか、国内でも、Cryptography Research and Evaluation Committees (CRYPTREC)の評価を元に作成された電子政府推奨暗号リストに含まれている。

3.2 Camellia

Camellia [9]は、NTTと三菱電機によって開発された共通鍵

暗号であり、Feistel 構造を採用したブロック暗号である。ブロック長は128 bit、鍵長は128, 192, 256 bitのいずれかを選択できる。ラウンド数は、128 bit 鍵の場合で18段、192 bit および256 bit の場合で24段である。Camelliaは、NESSIEや国内の電子政府推奨暗号リストに含まれている。

3.3 SEED

SEED [10]は、Korea Information Security Agency (KISA)によって開発された共通鍵暗号であり、Feistel 構造を採用したブロック暗号である。ブロック長は128 bit、鍵長は128 bitとなっている。ラウンド数は16段である。

3.4 Triple Data Encryption Algorithm (TDEA)

Triple Data Encryption Algorithm (TDEA) [11]は、DESを3回繰り返すことによって暗号強度を高める方式である。DESは共通鍵暗号であり、Feistel 構造を採用したブロック暗号である。ラウンド数は16段である。

TDEAでは、3回のDES暗号化/復号処理において、3つの異なる鍵を用いる場合と、2つの異なる鍵を用いる場合がある。なお、3回の処理で全て同一の鍵を用いるとSingle DESと同じ結果が得られるため、TDEAを採用したシステムでもDESとの互換性を保つことができる。ブロック長は64 bitであり、鍵長は、使用する鍵が1, 2, 3種類である場合にそれぞれ56, 112, 168 bitとなる。

3.5 MISTY1

MISTY1 [12]は、三菱電機によって開発された共通鍵暗号であり、Feistel 構造を採用したブロック暗号である。ブロック長は64 bitで、鍵長は128 bitである。ラウンド数は4の倍数の範囲で可変であり、8段とすることが推奨されている。MISTY1は、NESSIEや国内の電子政府推奨暗号リストの標準暗号として採用されている。

3.6 CAST-128

CAST-128 [13]はCarlisle Adamsによって開発された共通鍵暗号であり、Feistel 構造を採用したブロック暗号である。ブロック長は64 bitであり、鍵長は40~128 bitの範囲で8 bit単位で選択可能である。ラウンド数は、40~80 bitでは12段、88~128 bitでは16段となる。CAST-128は、Pretty Good Privacy (PGP)やIPsec等に採用されている。

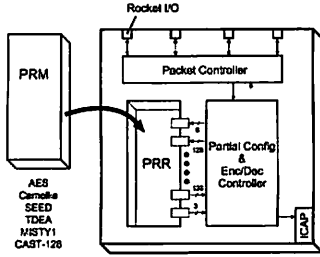


図4 PR-Cryptのブロック図

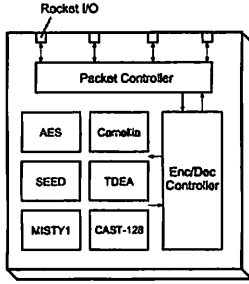


図5 NonPR-Cryptのブロック図

4 実 装

本章では、部分再構成を使用した場合としない場合の回路の構成について述べる。部分再構成を利用した回路をPR-Crypt、利用しない回路をNonPR-Cryptとして説明する。今回の実験で使用した6つの暗号モジュールは、東北大学青木研のCryptographic Hardware Project [14] で公開されているソースコードを使用した。ソースコードはVerilog-HDLによって記述されている。これらは従来、ASICをターゲットとして設計されたものであるが、デバイスに依存しない記述となっており、FPGAにも実装可能である。各暗号モジュールの詳細については、文献 [15] を参照されたい。

4.1 PR-Crypt

PR-Cryptのブロック図を図4に示す。6つの暗号モジュールはそれぞれ異なるPRMに実装されており、使用時にPRRにダウンロードされる。PRMとコントローラの間は、合計34個のスライスベース・バスマクロで接続されている。コントローラからPRMへは、128bitのデータと5bitの制御信号が送られる。コントローラからPRMへは、128bitのデータと3bitの制御信号が送られる。

4.2 NonPR-Crypt

NonPR-Cryptのブロック図を図5に示す。6つの暗号モジュールがすべて同時に実装されている。ただし、各モジュールにはイネーブル信号が接続されており、同時に動作するモジュールが1つであるよう制御される。

5 結 果

5.1 回路規模

AES, Camellia, SEED, TDEA, MISTY1, CAST-128の6つの暗

表2 PRRのハードウェア・リソース

LUT	FF	Slice	MULT18X18	RAMB16	TBUF
14,336	14,336	7,168	64	64	3,584

号モジュールを、部分再構成回路を利用した場合としない場合のそれぞれで実装した。使用したFPGAボードはレクセオン・テクノロジー社^(注2)のREX2で、XC2VP70FF1704-5が1つ搭載されている。論理合成、配置配線には、Xilinx ISE 9.1.02i_PR2の標準ツールを使用した。また、フロアプランには、PlanAhead 9.2.5を使用した。なお、論理合成や配置配線のオプションは、面積ではなく動作速度に対して最適化されるように設定した。PRRの領域は、Slice X30Y8とX79Y151を対角線の両端とする長方形領域(横50、縦144 Slice)とした。この領域に含まれるハードウェアリソースは、表2のようになる。

部分再構成を利用しなかった場合(NonPR-Crypt)、および部分再構成を使用した場合(PR-Crypt)のハードウェア使用量と遅延を表3と表4にそれぞれ示す。ここで、NonPR-Crypt、PR-CryptのSlice使用量をそれぞれ S_{nonpr} 、 S_{pr} と表すこととする。また、Static回路のSlice使用量を s_{static} とする。さらに、各暗号モジュールのSlice使用量を s_{aes} 、 $s_{camellia}$ 、...などと表し、そのうちの最大値を s_{max} と表す。表3が示すように、

$$S_{nonpr} = 15,866 \quad (1)$$

であり、実際にはXC2VP40に実装可能であることがわかる。また S_{pr} は、 $s_{max} = s_{cast128}$ であるから、

$$\begin{aligned} S_{pr} &= s_{static} + s_{max} \\ &= s_{static} + s_{cast128} \\ &= 1,653 + 4,937 = 6,590 \end{aligned} \quad (2)$$

であり、実際にはXC2VP20に実装可能であることがわかる。

5.2 消費電力

NonPR-CryptとPR-Cryptにおける消費電力を、ツールを用いて解析した。消費電力の解析では、実装可能な最小のデバイスを用いた。すなわち、NonPR-CryptはXC2VP40FF1152-5上に、PR-CryptはXC2VP20FF1152-5上に実装した。NonPR-CryptのフロアプランにはPlanAhead 9.2.5を使用した。PR-CryptのフロアプランにはPlanAhead 8.2.10を使用した。PlanAheadのバージョンが異なるのは、PlanAhead 9では、PRRに内蔵ハードコアプロセッサ(PowerPC)が含まれている場合に、Static ModuleとPRMのマージの段階でエラーが出るためである。これは、ツールのバグである可能性がある。XC2VP20を使用する場合は、必要なハードウェアリソースを確保しようとする、どうしてもPRRにPowerPCコアが含まれてしまう。

解析は、配置配線後のシミュレーションモデルに対して行われた。電力解析ツールには、Xilinx ISE 9.1.02i_PR2に付属のXpower Version J.32を使用した。アクティビティ・レートの入力

(注2)：(株)レクセオン・テクノロジーは、産業技術総合研究所の支援を受けて設立されたベンチャー企業である。

表3 NonPR-Cryptのハードウェア使用量と遅延

Slice	(%)	LUT	(%)	FF/Latch	(%)	Delay (ns)	Freq (MHz)
15,866	(48%)	28,624	(43%)	4,869	(7%)	39.952	25.030

表4 PR-Cryptのハードウェア使用量, 遅延, および部分再構成時間

Module	Slice	(%)	LUT	(%)	FF/Latch	(%)	Delay (ns)	Bitstream (kB)	Config Time @ 10MHz (msec)
Static	1,653	(4%)	1,811	(2%)	1,567	(2%)	15.783	-	-
AES	3,700	(11%)	6,139	(9%)	947	(1%)	18.479	608	34.2
Camellia	2,820	(8%)	4,682	(7%)	540	(1%)	23.116	590	33.2
SEED	2,389	(7%)	4,022	(6%)	472	(1%)	38.748	609	34.3
TDEA	1,109	(3%)	1,503	(2%)	326	(1%)	15.079	608	34.2
MISTY1	2,678	(8%)	4,297	(6%)	488	(1%)	39.437	562	31.7
CAST128	4,937	(14%)	8,159	(12%)	1,081	(1%)	39.877	452	25.5

表5 NonPR-Cryptの消費電力 (XC2VP40, 10 MHz)

暗号モード	Dynamic	Quiescent	Total
AES	29 [mW]	102 [mW]	131 [mW]
Camellia	34	102	136
SEED	24	102	126
TDEA	21	102	123
MISTY1	78	102	180
CAST128	80	102	182

表6 PR-Cryptの消費電力 (XC2VP20, 10 MHz)

暗号モード	Dynamic	Quiescent	Total	PR/NonPR (%)
AES	51 [mW]	72 [mW]	123 [mW]	93.9 (%)
Camellia	67	72	139	102.2 (%)
SEED	40	72	112	88.9 (%)
TDEA	12	72	84	68.3 (%)
MISTY1	83	72	155	86.1 (%)
CAST128	85	72	157	86.3 (%)

には Value Change Dump (VCD) ファイルを使用し, VCD ファイルの作成には Mentor Graphics 社の ModelSim SE 6.0c を使用した。

シミュレーションでは, Advanced Encryption Standard Algorithm Validation Suite (AESAVS) における, Variable Text Known Answer Test (VarTxt KAT) と Variable Key Known Answer Test (VarKey KAT) のテストベクタを使用した。今回のシミュレーションでは, 暗号化のみを行った。VarTxt KAT では, 秘密鍵 (128 bit) を “000...0h” に固定し, 異なる 128 ブロックのデータ (128 bit) を平文として与える。VarKey KAT では, 平文を “000...0h” に固定し, 異なる 128 個の秘密鍵について暗号化を行う。今回は, AES モジュールだけでなく, 他の暗号モジュールに対しても AESAVS のテストベクタを使用した。

なお, 実際のシステムでは高速シリアル I/O である Rocket I/O を使用してデータを入力するが, シミュレーション時のテストベクタの入力を容易にするために, 電力解析用の回路のトップデザインは, データが 32 bit 並列で入力されるように変更されている。ゆえに, 電力解析用の回路は実際に利用される場合とは入出力ピンの使用方法が異なるため, I/O の消費電力は含まず, コア ($V_{ccint} = 1.5$ [V]) の消費電力のみを考慮する。

NonPR-Crypt と PR-Crypt の消費電力を, 表 5 と表 6 にそれぞれ示す。また, 部分再構成実行時の消費電力は 89mW であった。

6 考 察

6.1 回路規模

本節では, 5.1 節で示したハードウェアリソース使用量をもとに, 部分再構成を利用した場合の回路規模の削減効果について議論する。5.1 節で示した Slice 使用量 $S_{nonpr} = 15,866$,

$S_{pr} = 6,590$ を用いると,

$$S_{pr}/S_{nonpr} = 6,590/15,866 = 0.415 \quad (3)$$

であるから, 理想的には, 部分再構成を利用することによってハードウェア使用量を 41.5% にまで削減できることがわかる。しかし現実には, リソース量が $s_{cast128}$ である PRR に対し, CAST-128 を配置配線することはできない。今回, 試行錯誤の結果, PRR を表 2 のように設定した。PRR が含むべきリソース量については, PRM のリソース使用量, PRR の形状, バスマクロの数や位置などに大きく依存すると考えられ, 研究の余地が残されている。今回, 実際に設定した PRR のリソース量 (s_{pr}) を使用すると,

$$S_{pr} = s_{static} + s_{pr} = 1,653 + 7,168 = 8,821. \quad (4)$$

となり, この場合も実装可能な最小デバイスが XC2VP20 となることがわかる。このとき,

$$S_{pr}/S_{nonpr} = 8,821/15,866 = 0.556 \quad (5)$$

であり, 部分再構成によってハードウェアリソース使用量は 55.6% にまで削減できることがわかる。

しかし FPGA では, 実際に使用するリソース量をいくら小さくしても, 用意されているリソース量はデバイスが変わらない限り一定である。ゆえに, 使用するデバイスそのものを小さくすることが重要である。今回の暗号モジュールの実装では, 部分再構成を利用することによって, デバイスを XC2VP40 から XC2VP20 にすることができた。これら 2 つのデバイスの比較を表 7 に示す。表 7 より, パッケージのサイズを小さくすることはできなかったが, デバイスの価格が 40% 以下に抑えられることがわかる。

表7 XC2VP40 と XC2VP20 の Slice 数と価格

	XC2VP40	XC2VP20	Ratio (%)
Slice	43,632	20,880	47.9%
最小パッケージ	FG676	FG676	-
パッケージサイズ (mm)	26x26	26x26	100%
価格	¥95,700	¥37,800	39.5%

6.2 消費電力

表5および表6が示すように、Camelliaを除く5つの暗号モジュールにおいて、部分再構成を利用することで消費電力を下げることができた。しかし、動的消費電力のみに注目すると、TDEAを除く5つの暗号モジュールにおいて、部分再構成を利用した方が消費電力が増えていることがわかる。静的消費電力は、全てのモジュールにおいて部分再構成を利用した方が30mW小さくなった。すなわち、部分再構成を利用することによる消費電力の低下は、デバイスが小さくなったことによる静的消費電力の削減の効果が大きい。

NonPR-Cryptの動的消費電力が比較的低い理由としては、イネーブル信号の利用が挙げられる。6つの暗号モジュールはすべて同時にFPGA上に実装されているが、イネーブル信号によって、それらの中の1つしか動作しないように設計されている。イネーブル信号を用いた場合、論理合成ツール(XST)はクロック・イネーブル付きのプリミティブを使って回路を実現するため、動作していないモジュールの動的消費電力は抑えられる。

PR-Cryptの動的消費電力が比較的高い理由としては、バスマクロの使用が挙げられる。PR-Cryptでは、PRMと固定回路は34個のバスマクロで接続されており、すなわち136個のLUTが使用されている。PRMへの入出力は必ずバスマクロを経由して行われるため、バスマクロ内のロジックのトグルレートは比較的高いと推測され、動的消費電力が高くなったと思われる。

消費電力を下げるためには、PRMとStatic回路間をできるだけ少ないバスマクロで接続することが必要であるといえる。しかし、バスマクロを少なくすると、PRMのスループットが低下する。要求された性能を満たすよう、PRMとStatic回路間のバスを設計する必要がある。

また、例えばAESで暗号化処理を行う場合を考える。表4より、AESモジュールは10MHzのもとで構築する場合に34.2msecの時間を要する。第5.2節で述べたように、部分再構成時の消費電力は89mWである。PR-CryptにAESモジュールを構築して暗号化処理を行う場合の消費電力量が、NonPR-Cryptの場合と等しくなる時間を求めると、

$$131 \cdot t = 123 \cdot t + 89 \cdot 34.2 \times 10^{-6} \quad (6)$$

より、 $t = 380.475 \times 10^{-6} = 380$ [msec] となる。すなわち、暗号化処理が380msec以上連続するようなアプリケーションではトータルの消費電力量を削減することができるが、これより短い時間間隔で部分再構成が行われる場合、消費電力量はむしろ増加することになる。

7 おわりに

本稿では、FPGAの動的部分再構成(Dynamic Partial Reconfiguration: DPR)を利用することで、回路規模や消費電力がどの程度削減されるかについて述べた。ISO/IEC 18033-3に採用されている6つの共通鍵ブロック暗号のモジュールを、DPRを利用した場合と利用しない場合において実装し、回路規模と消費電力を比較した。

DPRを利用した場合は、DPRを利用しない場合と比べて回路規模を約50%に抑えることができ、使用するデバイスをXC2VP40からXC2VP20へと小さくすることができた。これにより、デバイスのコストは40%以下にまで削減された。

DPRを利用する場合、使用するデバイスが小さくなるために静的消費電力を大きく下げることができるが、動的消費電力はむしろ増加した。これは、今回の実装では、Partially Reconfigurable Module (PRM)のスループットを大きくするために、34個ものバスマクロを利用したためと思われる。消費電力の削減を目指す場合は、PRMのスループットが要求を満たすよう配慮しながら、使用するバスマクロの数を減らす必要がある。また、暗号化処理が長時間連続して実行されるようなアプリケーションでなければ、消費電力量は削減されない。

今後の課題としては、PRMのスループットと消費電力のトレードオフの関係を明らかにすることが挙げられる。

文 献

- [1] ISO/IEC 18033-3, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, July 2005.
- [2] Xilinx, “Two flows for partial reconfiguration: Module based or difference based,” Sept. 9, 2004 2004.
- [3] Xilinx, Development System Reference Guide, for ISE8.1i edition, 2005.
- [4] 堀洋平, 横山浩之, 坂根広史, 戸田賢二, “FPGAの自己動的部分再構成利用したシステムの設計と開発,” 信学技報 RECONF2006-75, pp.61–68, 2006.
- [5] B. Jackson, Partial Reconfiguration Design with PlanAhead 9.2, Xilinx, Inc., Aug. 2007.
- [6] N. Dorairaj, E. Shiflet, and M. Goosman, “PlanAhead Software as a platform for partial reconfiguration,” Xcell Journal, vol.55, pp.68–71, 2005.
- [7] National Institute of Standards and Technology, “Announcing the advanced encryption standard (AES),” FIPS PUB 197, Nov. 2001.
- [8] U.S. Department of Commerce/National Institute of Standards and Technology, Data Encryption Standard (DES), fips pub 46-3 edition, 1999.
- [9] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, Specification of Camellia – a 128-bit Block Cipher Version 2.0, NTT and Mitsubishi Electric Corporation, Sept. 2001.
- [10] KISA, SEED Algorithm Specification, .
- [11] NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, sp 800-67 edition, May 2004.
- [12] M. Matsui, Specification of MISTY1 – a 64-bit Block Cipher, NESSIE Project.
- [13] C. Adams, The CAST-128 Encryption Algorithm, May 1997.
- [14] “Cryptographic hardware project,” <http://www.aoki.ecei.tohoku.ac.jp/crypto/> Aoki Lab., Tohoku University.
- [15] T. Sugawara, N. Homma, T. Aoki, and A. Satoh, “ASIC performance comparison for the ISO standard block ciphers,” JWS 2007, pp.485–498, Aug. 2007.