情報処理学会論文誌　コンピューティングシステム　Vol. 1　No. 2　47–58 (Aug. 2008)

FPGA の動的部分再構成を用いたマルチ暗号モジュールの回路規模と消費電力の削減

堀　洋平[†1]　坂根広史[†1]
片下敏宏[†1]　戸田賢二[†1]

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る実装による，回路面積と消費電力の削減効果を評価した．FPGA には，回路の一部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を削減することができると期待されている．今回，5 つの標準的な暗号モジュール（AES，Camellia，SEED，TDEA，MISTY1）を用い，これらを同時に実装した場合と，1 つずつ切り替えて再構成した場合のリソース使用量と消費電力を評価した．その結果，FPGA の部分再構成を利用することで，回路規模は約 65% 削減され，実行時消費電力は最大で約 40%，待機電力は最大で 53 %以上低減させることができた．

Area and Power Reduction with Dynamic Partial Reconfiguration of Multi-Algorithm Cryptographic Modules

Yohei Hori,[†1] Hirofumi Sakane,[†1]
Toshihiro Katashita[†1] and Kenji Toda[†1]

We evaluated the effectiveness of dynamic partial reconfiguration in reducing area and power consumption of an FPGA-based circuit. We implemented 5 cryptographic modules (AES, Camellia, SEED, TDEA, and MISTY1) on the partially reconfigurable and non-reconfigurable circuits. Using dynamic partial reconfiguration, the area of the circuit is reduced by about 65% and the power consumption during operation and standby are reduced by at most 40% and 53%, respectively.

†1 独立行政法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)

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民生機器にも幅広く搭載されるようになった．FPGA には，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ものがあり，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を実現できる．また，1 つの領域を複数のモジュールを切り替えながら使用することができるため，実装面積や消費電力の削減が期待できる[4]．

これまで，1 つのアプリケーションを異なる回路規模のアーキテクチャで実現し，これらを DPR を用いて切り替えて消費電力を削減する手法が報告されている[13]．たとえば，要求スループットが高い場合は消費電力が大きく大規模な回路を実装し，要求スループットが低くなると低消費電力で小規模な回路に切り替えるといった具合である．これは，同一アプリケーションにおける「アーキテクチャ切替え型」の DPR システムである．

一方，DPR を用いて複数のアプリケーションを切り替え，回路を小型化するのが「アプリケーション切替え型」の DPR システムである．たとえば，複数の標準暗号アルゴリズムに対応した組み込み向け LSI では，アルゴリズムごとに専用のモジュールを搭載しているが，同時に動作するモジュールは通常 1 つであるため，それらを切り替えて使用することになる．この場合，DPR を用いることで大幅な回路規模削減が可能であり，消費電力の削減も期待できる．しかしアプリケーション切替え型の DPR システムの場合，ある時点で処理を行っているロジックの面積は非 DPR システムとほぼ等しいか，むしろ DPR に固有の制御の分だけ大きくなることも考えられるため，動的消費電力の削減効果は明らかでない．また，DPR による回路の切替え処理も動的電力を消費するため，回路の小型化による静的消費電力の低下と，DPR による動的消費電力の増加の双方を評価する必要がある．このようなアプリケーション切替え型の DPR システムにおける省電力効果を実測によって定量的に評価した研究は，筆者らの知る限り報告されていない．

本研究では，ISO/IEC 18033 標準[5] である共通鍵暗号アルゴリズム AES，Camellia，SEED，TDEA，MISTY1 を FPGA に実装し，アプリケーション切替え型 DPR の回路規模と消費電力の削減効果の評価実験を行った．その結果，DPR により回路規模と消費電力がともに削減されることが明らかとなった．

2. 関 連 研 究

Noguera らは，Xilinx 社の Virtex-II Pro[21] の DPR 機能を利用することで，Viterbi デコーダの消費電力を削減している[13]．Viterbi デコーダは，拘束長 k によって Bit Error Rate（BER）が大きく変化する．k を大きくすると BER は改善されるが，回路規模は大きくなる．そこで，BER が大きくてもかまわない場合には，回路規模の小さな Viterbi デコーダを実装して消費電力を抑えることができる．Noguera らの研究は，アプリケーションは Viterbi デコーダに固定であるため，アーキテクチャ切替え型の DPR である．Noguera らの研究では，切り替える回路の規模に最大で 10 倍の開きがあり，本研究のように同程度の回路規模の複数アプリケーションを切り替える場合と異なる．またこの研究は，同一チップ上における DPR システムどうしの比較であるため，DPR に固有のオーバヘッドは考慮されていない．

Lorenz らは Atmel 社の AT40K20[2] を使い，データ幅の異なる乗算器を構築する際の消費電力を実測によって求め，DPR を用いた省電力効果について論じている[8]．しかし，Lorenz らは静的消費電力と DPR 時の消費電力を測定したにすぎず，演算中の動的消費電力は部分再構成システムと非部分再構成システムで同じであると仮定している．また，切り替えるモジュールの数を N とするとき，非部分再構成システムの静的消費電力を単純に部分再構成システムの N 倍で見積もっている．さらに DPR 時の消費電力は，再構成の前後のモジュールによって変わると考えられるが，Lorenz らはこれを一定として議論している．

そこで本研究は，DPR システムの動作中および再構成中の消費電力を実測によって求め，アプリケーション切替え型 DPR の省電力効果について議論する．

3. FPGA の動的部分再構成

DPR をサポートする FPGA には，Xilinx 社の Virtex シリーズと Spartan シリーズ，および Atmel 社の AT40 シリーズと AT94 シリーズがあるが，今回は Xilinx FPGA を用いている．本研究では，Early Access Partial Reconfiguration（EA PR）[20] と呼ばれる最新の方法で部分再構成を行っており，EA PR は旧来手順[18),19)] における制約の緩和により設計の効率が飛躍的に向上している．

3.1 DPR 対応 FPGA

Xilinx FPGA の DPR 対応状況について，**表 1** にまとめる[⋆1]．部分再構成に対応している Spartan および Virtex シリーズのうち，Virtex シリーズは動的再構成に，さらに Virtex-II 以降のデバイスは自己再構成に対応している．本研究では Virtex-II Pro を使用しているため，以下では単に部分再構成と記述した場合も動的部分再構成（DPR）をさすものとする．

表 1　Xilinx FPGA の部分再構成対応状況
Table 1　RTR availability of Xilinx FPGAs.

Device	発売年	部分再構成	動的再構成	自己再構成
Virtex	1998	○ (untested)	○ (untested)	×
Virtex-E	1999	○ (untested)	○ (untested)	×
Virtex-II	2000	○	○	○
Virtex-II Pro/-II ProX	2002/2003	○	○	○
Virtex-4	2004	○	○	○
Virtex-5	2006	○	○	○
Spartan	1998	○ (untested)*	× (untested)	×
Spartan-II/-IIE	1999/2001	○*	×	×
Spartan-3/-3L/-3E	2003/2004/2005	○	×	×
Spartan-3A	2006	○	×	×

∗ 現時点ではバスマクロが提供されていない．

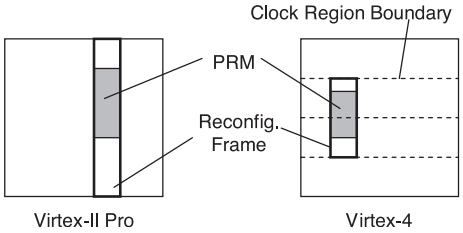

図 1　部分再構成フレーム
Fig. 1　Outline of a partially reconfigurable frame.

3.2 部分再構成モジュール

EA PR 回路では，長方形のモジュール単位で DPR を行う．このとき，DPR 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．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

⋆1 2006 年 12 月の時点の対応状況．E-mail による Xilinx との私信に基づく．2006 年 12 月 13–15 日．

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リージョンの境界に等しい（図 1 右）．

3.3 バスマクロ

DPR では，再構成後の回路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 の入出力信号は，クロック等のグローバル信号を除き，必ずバスマクロを通らなければならない．バスマクロの位置をつねに一定にすることで，DPR 後の信号が確実に結線される．

3.4 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 を利用することで，自己再構成が可能となる．

4. 共通鍵ブロック暗号

本章では，ISO/IEC 18033-3 で採用された共通鍵ブロック暗号のうち，本研究で実装した AES，Camellia，SEED，TDEA，MISTY1 の概要について説明する．

4.1 Advanced Encryption Standard（AES）

Advanced Encryption Standard（AES）[10] は，危殆化が懸念される Data Encryption Standard（DES）[17] に代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．

4.2 Camellia

Camellia [1] 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．

4.3 SEED

SEED [7] 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．

4.4 Triple Data Encryption Algorithm（TDEA）

Triple Data Encryption Algorithm（TDEA）[12] 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 回の処理ですべ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．

4.5 MISTY1

MISTY1 [9] 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．

5. 実　　装

本章では，消費電力の評価を行った環境と，実装した回路の詳細について説明する．

5.1 評 価 環 境

暗号回路の消費電力を実測するため，FPGA ボードとして SASEBO（Side-channel Attack Standard Evaluation BOard）[14),⋆1] を使用した．SASEBO は，暗号の電力解析攻撃の評価を目的として作成されたボードで，FPGA の消費電力を測定するのに適している．SASEBO には，Xilinx 社製 FPGA である XC2VP7-FG456-5 と XC2VP30-FG676-5 が搭載されている．以下では，これらの FPGA をそれぞれ XC2VP7，XC2VP30 と表記する．2 つの FPGA へのクロック系統は独立しており，今回はともに 24 MHz のクロックを供給した．FPGA コアの電源電圧はともに 1.5 V で，それぞれの電源ラインには 1 Ω のシャント抵抗が実装されている（**図 2**）．

コア電圧を V_{ccint}，シャント抵抗の抵抗値を R，シャント抵抗の両端の電位差を V_r とすると，FPGA コアの消費電力 P は，

⋆1 SASEBO は経済産業省の委託事業の中で，産業技術総合研究所と東北大学が共同で開発した，暗号モジュールのサイドチャネル攻撃実験用標準評価 FPGA ボードである．

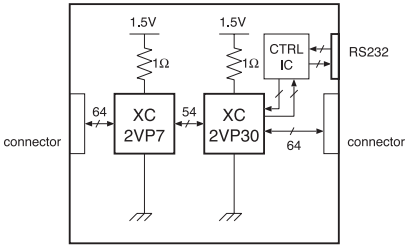

図 2　SASEBO の概略図
Fig. 2　Outline of SASEBO.

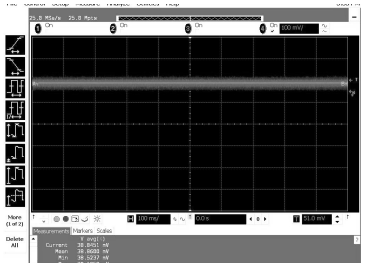

図 3　オシロスコープによる電圧波形の取得
Fig. 3　Wave data acquired by the oscilloscope.

$$P = V_{ccint} \cdot \frac{V_r}{R} \tag{1}$$

により求めることができる．すでに述べたように，$V_{ccint} = 1.5\,[\mathrm{V}]$，$R = 1\,[\Omega]$ である．シャント抵抗の両端の電位差 V_r は，オシロスコープを用いて測定した．本研究では，アジレント社製のオシロスコープ DSO8104A（帯域幅 1 GHz，4 GSa/s），差動プローブ 1130A（帯域幅 1.5 GHz），およびプローブヘッド E2695A を使用した．このオシロスコープには，取得した波形の平均値を算出する機能が搭載されている．

暗号化処理時の消費電力は，次のようにして求められる．まず，暗号化処理を実行中の任意の時点から，オシロスコープによる電圧波形の取得を開始する．波形取得時のオシロスコープのパラメータは 25.0 MSa/s であり，1 秒間の波形中の 2,500 万サンプリングポイントの平均電圧を算出する．1 秒間に実行される暗号化処理の回数は十分に大きいため，処理中の任意の時点から電圧波形を取得しても問題はない．**図 3** に，オシロスコープを用いて

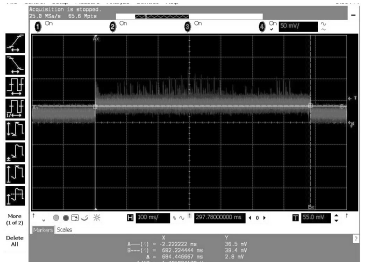

図 4　部分再構成時の電圧波形の取得
Fig. 4　Wave data acquired by the oscilloscope during DPR.

取得された波形の例を示す．このようにして電圧を取得する操作を 10 回繰り返し，その平均値を V_r とする．この値を用いて，式 (1) より消費電力を求めることができる．

また DPR 時の消費電力も，同様にオシロスコープを用いて V_r を取得することで求める．DPR は，待機中に Xilinx Parallel Cable IV を用いて PRM のビットストリームを入力することで行う．**図 4** に，DPR 時に取得された電圧波形の例を示す．待機中に DPR を行うと，図 4 のように電圧波形が不連続に変化する．この波形の立ち上がりを DPR の開始，立ち下がりを終了時点とみて，DPR 中の電圧の平均値をオシロスコープの機能を用いて算出する．

5.2　暗号回路の実装

4 章で述べた暗号モジュールを，部分再構成を利用する場合としない場合の 2 つのパターンで実装した．今回の実験で使用した暗号モジュールは，東北大学の Cryptographic Hardware Project [3] 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．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．以下，DPR を利用する回路を **PR-Crypt**，DPR を利用しない回路を **NonPR-Crypt** と呼ぶ．

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，PR-Crypt のフロアプランには Xilinx PlanAhead 8.2.10 [6] を使用した．

5.2.1　PR-Crypt

PR-Crypt は SASEBO 上の XC2VP7 に実装される．**図 5** に PR-Crypt のブロック図を示す．PR-Crypt には PRR が 1 つあり，ここに 5 種類の PRM（AES，Camellia，SEED，TDEA，MISTY1）のうち 1 つが構築される．PRM の転送には Parallel Cable IV を使用し，Boundary Scan（JTAG）インタフェースから DPR を行った．

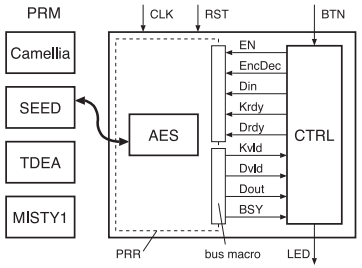

図 5　PR-crypt のブロック図
Fig. 5　Block diagram of PR-Crypt.

表 2　PRM への入出力信号
Table 2　Inputs and outputs of the PRM.

信号	方向	幅 (bit)	説明
Din	in	128	平文/暗号文，鍵データ入力
RSTn	in	1	リセット信号
EN	in	1	イネーブル信号
EncDec	in	1	0=暗号化，1=復号
Krdy	in	1	鍵データレディ
Drdy	in	1	平文/暗号文レディ
Dout	out	128	平文/暗号文出力
Kvld	out	1	鍵データ有効フラグ
Dvld	out	1	平文/暗号文の有効フラグ
BSY	out	1	暗号化/復号の実行中フラグ

PRM と固定領域は，34 個のバスマクロを通じて接続されている．PRM への入出力信号を**表 2** に示す．なお，Din，Dout の 128 bit の幅のバスは，PRM として MISTY1（64 bit データ）や TDEA（56 bit 鍵，64 bit データ）が実装されている場合は，必要な幅のみ使用される．PRR は，Slice X0Y8-X59Y63 の範囲に設定した．PRR が含むハードウェアリソース量は**表 3** のようになっており，デバイス全体の約 66%を占める．

モジュール CTRL は，PRM へのテストデータや制御信号の生成を行う．テストデータは，Advanced Encryption Standard Algorithm Validation Suite（AESAVS）[11] における，Variable Text Known Answer Test（VarTxt KAT）の値を使用した．すなわち，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）を平文として与えたときの暗号化時の消費電力を測定した．また，AES モジュールだけでなく，他の

表 3　PRR のハードウェア・リソース
Table 3　Hardware resource of PRR.

LUT	FF	Slice	MULT	RAMB	TBUF
6,656	6,656	3,328	32	32	1,664

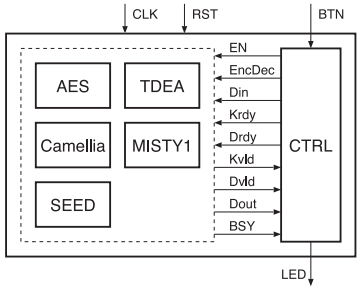

図 6　NonPR-crypt のブロック図
Fig. 6　Block diagram of NonPR-Crypt.

暗号モジュールに対しても AESAVS のテストベクタを入力として与えた．ただし TDEA，MISTY1 においては，これらのテストベクタの上位 64 bit を使用した．

なお，暗号モジュールはどのような平文や鍵の入力に対しても処理結果に統計的な偏りがほとんど見られないよう設計されているため，鍵を 0 に固定した場合とその他の鍵を使用する場合で消費電力はほぼ変わらない．ゆえに，秘密鍵を 0 に固定することに問題はない．

PR-Crypt には待機モードと実行モードが存在する．待機モードは，暗号処理が行われていない状態であり，外部から暗号処理開始のトリガを待っている状態である．実行モードでは 128 個の平文が繰り返し入力され，暗号化処理は各モジュールに固有のサイクル数で連続して行われる．AES，Camellia，SEED，TDEA および MISTY1 における暗号化処理のサイクル数はそれぞれ，15，28，20，53，13 である．

5.2.2　NonPR-Crypt

NonPR-Crypt は SASEBO 上の XC2VP30 に実装される．**図 6** に NonPR-Crypt のブロック図を示す．NonPR-Crypt には 5 個の暗号モジュールがすべて実装されるが，同時に動作するモジュールは 1 個となるようイネーブル信号によって制御されている．NonPR-Crypt は外部からのトリガによって，待機モードおよび AES，Camellia，SEED，TDEA，MISTY1 の各暗号化処理モードを順に遷移するようになっている．モジュール CTRL は

PR-Crypt の場合と同様に，暗号モジュールへのテストデータや制御信号の生成を行う．テストデータも PR-Crypt と同様に，AESAVS の VarTxt KAT の入力ベクタを使用した．また，消費電力の測定も，PR-Crypt と同様の方法でオシロスコープを用いて行った．

6. 結　　果

6.1 回 路 規 模

NonPR-Crypt のハードウェアリソース使用量を**表 4** に示す．NonPR-Crypt の Slice 使用量は 9,616 であり，これは XC2VP30 の 70% にあたる．また，PR-Crypt のハードウェアリソース使用量を**表 5** に示す．表 5 中の Static は，部分再構成を行わない固定回路である．5 個の PRM のうち回路規模が最大のものは AES であった．PR-Crypt では同時に構築される PRM はたかだか 1 個であるから，PR-Crypt のリソース使用量の最大値は，Static と AES のリソース使用量の合計となる．すなわち，PR-Crypt のハードウェアリソース使用量は 3,387（= 411 + 2,976）となる．

6.2 消 費 電 力

表 6 に，NonPR-Crypt における各暗号モジュールの暗号化処理時の消費電力と，スループットを示す．また，**表 7** に各暗号モジュールを実装した PR-Crypt におけるスループット，消費電力，および消費電力の NonPR-Crypt との比率を示す．実装された回路は，NonPR-Crypt，PR-Crypt ともに 24 MHz で動作した．また，DPR を用いることによる各暗号モジュールの処理サイクル数への影響はないため，暗号化処理のスループットは 2 つの回路で変わらない．

表 8 に，PR-Crypt における DPR の消費電力を示す．今回の実験では，ボードから水晶発振子を取り除いた状態で電圧を印加することで，FPGA の静的消費電力も求めた．表中において “待機時” とは，ロジックへのクロックの供給は行われているが，暗号化処理が実行

表 4　NonPR-Crypt のハードウェア使用量
Table 4　Hardware utilization of NonPR-Crypt.

Slice	(%)	LUT	(%)	FF	(%)
9,616	(70%)	18,177	(66%)	2,454	(8%)

表 5　PR-Crypt のハードウェア使用量，ビットストリームサイズ，および部分再構成時間
Table 5　Hardware utilization, bitstream size, and configuration time of PR-Crypt.

Module	Slice	(%)	LUT	(%)	FF	(%)	Partial bitstream	Config time
Static	411	(8%)	231	(2%)	174	(1%)	-	-
AES	2,976	(60%)	4,752	(48%)	945	(9%)	313.974 kB	675.11 msec
Camellia	2,308	(46%)	3,729	(37%)	530	(5%)	314.366 kB	673.78 msec
SEED	2,389	(48%)	4,019	(40%)	472	(4%)	310.354 kB	682.00 msec
TDEA	1,122	(22%)	1,503	(15%)	326	(3%)	293.838 kB	628.89 msec
MISTY1	2,674	(54%)	4,290	(43%)	488	(4%)	315.614 kB	675.33 msec

表 6　NonPR-Crypt の暗号化時の消費電力
Table 6　Power consumption of NonPR-Crypt.

	Thr'put	消費電力 [mW]		
	[Mbps]	静的	動的	合計
待機時	-	32.290	38.718	71.008
AES	204.8	32.290	303.819	336.109
Camellia	109.7	32.290	263.053	295.343
SEED	153.6	32.290	515.973	548.263
TDEA	28.98	32.290	67.771	100.061
MISTY1	118.2	32.290	390.529	422.819

（XC2VP30，24 MHz）

表 7　PR-Crypt の暗号化時の消費電力
Table 7　Power Consumption of PR-Crypt during the encryption process.

	Thr'put	待機時消費電力 [mW]				実行時消費電力 [mW]			
実装 PRM	[Mbps]	静的	動的	合計	削減率 (%)	静的	動的	合計	削減率 (%)
AES	204.8	23.157	17.052	40.209	(43.4)	23.157	299.369	322.526	(4.04)
Camellia	109.7	23.157	14.709	37.866	(46.7)	23.157	205.735	228.892	(22.4)
SEED	153.6	23.157	13.794	36.951	(47.8)	23.157	490.727	513.884	(34.4)
TDEA	28.98	23.157	9.753	32.910	(53.7)	23.157	37.004	60.161	(39.9)
MISTY1	118.2	23.157	13.852	37.009	(47.9)	23.157	397.279	420.436	(0.574)

（XC2VP7，24 MHz）

表 8　PR-Crypt の部分再構成時の消費電力
Table 8　Power Consumption of PR-Crypt during the partial reconfiguration.

from \ to	AES [mW]	Camellia [mW]	SEED [mW]	TDEA [mW]	MISTY1[mW]
AES	33.886	74.665	103.614	47.282	117.256
Camellia	88.478	33.046	116.632	46.208	86.802
SEED	75.957	50.145	31.845	44.392	58.991
TDEA	57.481	43.370	71.674	34.434	55.404
MISTY1	51.179	53.271	117.791	46.704	32.203

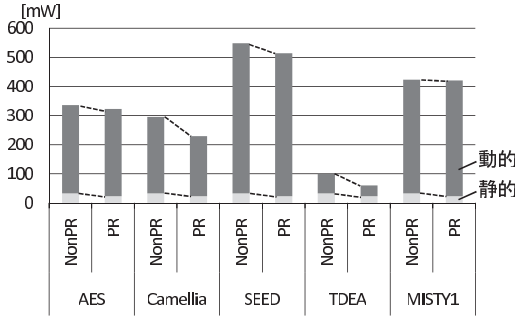

図 7　暗号化処理時の消費電力
Fig. 7　Power consumption during data encryption.

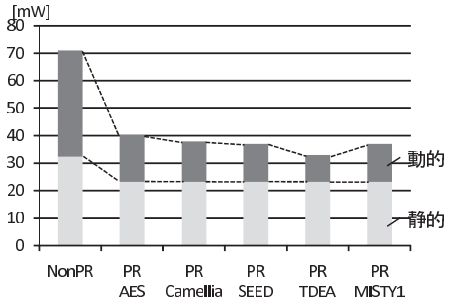

図 8　待機時の消費電力
Fig. 8　Power consumption during standby.

されいない状態である．**図 7**，**図 8** はそれぞれ，実行時と待機時の消費電力の比較である．

7. 考　　察

7.1　回路規模削減効果

6.1 節の結果より，NonPR-Crypt の Slice 使用量は 9,616，PR-Crypt は 3,387 であった．ゆえに，部分再構成を用いた場合のリソース使用量の削減率は，

$$\frac{9{,}616 - 3{,}387}{9{,}616} = 0.648 \tag{2}$$

と求められ，必要なリソース量を 64.8%削減することができた．

表 9　XC2VP30 と XC2VP7 の比較
Table 9　Comparison of XC2VP30 and XC2VP7.

	XC2VP30	XC2VP7	削減率 (%)
Slice	13,696	4,928	64.0%
Size (mm)	26 × 26	23 × 23	21.7%

FPGA を民生機器等に搭載する場合は，どの程度デバイスを小さくできるかが重要である．今回の暗号回路では，使用するデバイスを XC2VP30 から XC2VP7 へと小型化することができた．**表 9** は，今回使用した XC2VP30 と XC2VP7 の比較である．表 9 が示すように，搭載 Slice 量の少ないデバイスを採用することが可能になり，パッケージのサイズも 21.7%小さくすることができた．以上のことから，部分再構成を利用することによって製品の小型化が可能であり，さらに製品の軽量化や低価格化が期待できるといえる．

7.2　消費電力削減効果

表 6 および表 7 が示すように，部分再構成を利用した PR-Crypt の方が，NonPR-Crypt よりも消費電力を抑えることができた．特に，静的消費電力が小さくなったため，待機電力は NonPR-Crypt と比べて 43%から 54%削減することができた．XC2VP7 と XC2VP30 の静的消費電力の差は約 9 mW であり，待機電力の削減量はそれよりも大きいが，これは待機中のロジックの面積が削減されたためと考えられる．待機中のモジュールもクロックは供給されているため，ある程度の動的電力を消費している．NonPR-Crypt では 5 個の暗号モジュールが実装されており，このうち実行中のものはたかだか 1 個で残りは待機中であるが，DPR システムでは実行される暗号モジュール 1 個のみ実装されるため，待機中のロジックの面積は大幅に縮小される．DPR システムでは DPR の制御回路が動的電力を消費するが，そのオーバヘッドよりも待機中ロジックの動的消費電力を削減できたことの効果が大きかったといえる．

以下では，DPR を用いた FPGA の消費電力削減効果について，実行時電力と待機電力の観点からさらに詳しく論じる．

7.2.1　実行時電力

NonPR-Crypt における実行時消費電力，待機電力をそれぞれ P_r，P_w とし，PR-Crypt における実行時消費電力，待機電力，部分再構成時電力をそれぞれ P'_r，P'_w，P'_{conf} とおく．また，NonPR-Crypt に外部メモリがある場合，このメモリの待機消費電力と読み出し時の消費電力をそれぞれ P_{mw}，P_{mrd} とおく．同様に PR-Crypt に外部メモリがある場合，このメモリの待機消費電力と読み出し時の消費電力をそれぞれ P'_{mw}，P'_{mrd} とおく．暗号

化処理時間，待機時間，再構成時間をそれぞれ t_r，t_w，t_{conf} とすると，NonPR-Crypt と PR-Crypt における消費電力量 W および W' は以下のように表される．

$$W = (P_r + P_{mw}) \cdot t_r + (P_w + P_{mw}) \cdot t_w \tag{3}$$

$$W' = (P'_r + P'_{mw}) \cdot t_r + (P'_w + P'_{mw}) \cdot t_w + (P'_{conf} + P'_{mrd}) \cdot t_{conf}. \tag{4}$$

本項では暗号処理実行時の消費電力を考えるため，$t_w = 0$，すなわち暗号化処理が連続して実行され，待機時間がない場合の消費電力について考える．PR-Crypt の方が省電力であるためには，

$$W > W' \tag{5}$$

が成立する必要がある．式 (3)，(4) および $t_w = 0$ より式 (5) は，

$$(P_r + P_{mw}) \cdot t_r > (P'_r + P'_{mw}) \cdot t_r + (P'_{conf} + P'_{mrd}) \cdot t_{conf} \tag{6}$$

と表される．多くのシステムでは DPR の使用の有無にかかわらず外部メモリを搭載していると考えられる．この場合，NonPR-Crypt と PR-Crypt は同型のメモリを搭載していると考えられるため，

$$P_{mw} = P'_{mw} \quad \text{かつ} \quad P_{mrd} = P'_{mrd} \tag{7}$$

となる．表 7 より，すべての暗号モジュールにおいて $P_r > P'_r$ であるから，式 (6) は式 (7) を用いることによって，

$$t_r > \frac{P'_{conf} + P'_{mrd}}{P_r - P'_r} \cdot t_{conf} \tag{8}$$

と表される．

一方で，NonPR-Crypt は外部メモリを搭載せず，PR-Crypt のみ PRM のビットストリームを格納するために外部メモリが必要となる場合が考えられる．このとき，

$$P_{mw} = 0 \quad \text{かつ} \quad P_{mrd} = 0 \tag{9}$$

であるから，式 (6) は以下のように変形される．

$$\{P_r - (P'_r + P'_{mw})\} \cdot t_r > (P'_{conf} + P'_{mrd}) \cdot t_{conf}. \tag{10}$$

ここで，PRM のビットストリームをすべて格納するために，外部メモリとして 4-Mbit の Flash メモリ TC58FVT004[16] を用いる場合を考える．この Flash メモリの CMOS レベルにおける平均的な待機電流は 10 μA，読み出し時の電流は 30 mA であるから，電源電圧を 3 V とすると，

$$P'_{mw} = 0.030 \text{ [mW]} \tag{11}$$

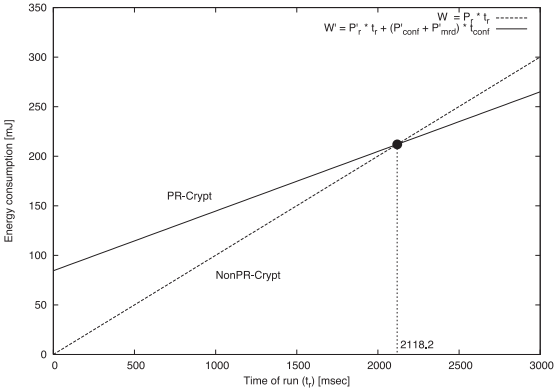

図 9　TDEA 実行時の消費電力量
Fig. 9　Energy consumption during TDEA operation.

$$P'_{mrd} = 90 \text{ [mW]} \tag{12}$$

となる．よって式 (10) において，P'_{mw} は P'_r に対して十分に小さいため問題なく無視することができる．また表 7 より，$P_r - (P'_r + P'_{mw})$ が負となる場合は存在しないため，式 (10) は，

$$t_r > \frac{P'_{conf} + P'_{mrd}}{P_r - P'_r} \cdot t_{conf} \tag{13}$$

と変形される．すなわち，外部メモリの待機電力が無視できる場合には式 (8) と等しくなることが分かる．

たとえば，実行時消費電力の削減効果の最も大きかった TDEA について考える．NonPR-Crypt における TDEA 暗号化時の消費電力は表 6 より 100.061 mW であり，PR-Crypt では表 7 より 60.161 mW である．また表 8 より，DPR によって TDEA を構築する際の消費電力の最小値は，SEED 実装時から TDEA に再構成する場合の 44.392 mW であり，再構築に要する時間は表 5 より 628.89 msec である．式 (13) より，

$$t_r > \frac{44.392 + 90}{100.061 - 60.161} \cdot 628.89 = 2118.2 \tag{14}$$

であるから，暗号化処理が約 2.1 秒以上連続する場合に，PR-Crypt の消費電力量は NonPR-Crypt を下回ることが分かる（**図 9**）．

同様に，消費電力の削減効果のワーストケースであった MISTY1 の消費電力量を考える．DPR によって MISTY1 を構築する際の消費電力の最大値は，AES 実装時から MISTY1

に再構成する場合の 117.256 mW であり，再構築に要する時間は 675.33 msec である．このとき，式 (13) より，

$$t_r > \frac{117.256 + 90}{422.819 - 420.436} \cdot 675.33 = 58735 \tag{15}$$

であるから，暗号化処理時間が約 59 秒以上連続する場合に，PR-Crypt の消費電力量が Non-PR を下回ることが分かる．

ストリーミング動画や音楽等の暗号化コンテンツでは，暗号化処理が連続する時間はこれらの値よりも十分に長いと考えられるため，部分再構成によって消費電力の低減が可能である．

7.2.2 待機電力

実際のアプリケーションでは，暗号化処理の実行時間よりも待機時間の方が長いと考えられる．ここでは，待機電力の削減による省電力効果について考える．

PR-Crypt の方が省電力であるためには，式 (3)，(4)，(5) より，

$$\begin{aligned}&\{(P_w + P_{wm}) - (P'_w + P'_{mw})\} \cdot t_w \\ &\quad > \{(P'_r + P'_{mw}) - (P_r + P_{mw})\} \cdot t_r \\ &\qquad + (P'_{conf} + P'_{wrd}) \cdot t_{conf}.\end{aligned} \tag{16}$$

NonPR-Crypt と PR-Crypt がともに同型の外部メモリを搭載しているとき，式 (7) より，

$$\begin{aligned}&(P_w - P'_w) \cdot t_w \\ &\quad > (P'_{conf} + P'_{wrd}) \cdot t_{conf} - (P_r - P'_r) \cdot t_r.\end{aligned} \tag{17}$$

表 7 よりすべての暗号モジュールにおいて $P_w > P'_w$ であるから，

$$t_w > \frac{(P'_{conf} + P'_{wrd}) \cdot t_{conf} - (P_r - P'_r) \cdot t_r}{(P_w - P'_w)}. \tag{18}$$

一方，PR-Crypt のみが外部メモリを搭載している場合，式 (9) を用いて式 (16) を変形すると，

$$\begin{aligned}&\{P_w - (P'_w + P'_{mw})\} \cdot t_w \\ &\quad > \{(P'_r + P'_{mw}) - P_r\} \cdot t_r + (P'_{conf} + P'_{wrd}) \cdot t_{conf}.\end{aligned} \tag{19}$$

7.2.1 項と同様に外部メモリとして TC58FVT004 を用いる場合，P'_{mw} は P'_w や P'_r に比べて十分に小さいため，問題なく無視できる．よって式 (19) は

$$t_w > \frac{(P'_{conf} + P'_{wrd}) \cdot t_{conf} - (P_r - P'_r) \cdot t_r}{(P_w - P'_w)} \tag{20}$$

と変形され，外部メモリの待機電力が無視できる場合は式 (18) と等しくなることが分かる．

表 10　Camellia + SEED + TDEA の暗号化時の消費電力
Table 10　Power consumption of the non-PR circuit with Camellia, SEED and TDEA.

	Thr'put	Camellia + SEED + TDEA			PR-Crypt	
	[Mbps]	静的 [mW]	動的 [mW]	合計 [mW]	合計 [mW]	削減率 (%)
待機時	-	23.157	29.6477	52.8047		
Camellia	109.7	23.157	219.8415	242.9985	228.892	(5.81)
SEED	153.6	23.157	516.423	539.580	513.884	(4.76)
TDEA	28.98	23.157	55.0191	78.1761	60.161	(23.0)

（XC2VP7，24 MHz）

今回の実験結果ではつねに $P_r > P'_r$ であるから，$t_r = 0$ のとき式 (18)，(20) 右辺の分子は最大となる．すなわち，部分再構成した PRM で暗号化処理がまったく実行されない場合，DPR 時の消費電力のオーバヘッドの影響が最大となる．このとき，

$$t_w > \frac{(P'_{conf} + P'_{wrd})}{(P_w - P'_w)} \cdot t_{conf}. \tag{21}$$

省電力効果のワーストケースである MISTY1 の場合で，$t_r = 0$ の場合ついて考える．MISTY1 での測定結果を式 (21) に適用すると，

$$t_w > \frac{117.256 + 90}{71.008 - 37.009} \cdot 675.33 = 4116.8 \tag{22}$$

となる．ゆえに待機時間が約 4.1 秒以上連続するならば，PR-Crypt の方が消費電力量は小さくなることが分かる．実際のアプリケーションでは，待機時間はこれよりも十分に長いと考えられるため，待機電力の小さな PR-Crypt は，消費電力の削減効果が大きいといえる．

7.3 同一デバイスによる比較

静的消費電力の削減を除いた DPR の省電力効果を確かめるため，DPR を利用せずに 3 つの暗号モジュールを XC2VP7 に実装し，PR-Crypt と消費電力を比較した．暗号モジュールを 3 個選ぶ組合せのうち，Camellia，SEED，TDEA および Camellia，MISTY1，TDEA の組合せのみが XC2VP7 に実装可能であった．これらの実装結果を**表 10**，**表 11** に示す．なお，実装された回路は 24 MHz で動作し，各暗号モジュールのスループットは NonPR-Crypt や PR-Crypt の場合と変わらない．

PR-Crypt は XC2VP7 上の非 DPR 回路 2 つと比較し，Camellia，SEED，TDEA 実行時の消費電力が低いことが示された．ただしその省電力効果は，PR-Crypt と NonPR-Crypt を比較対象とした場合よりも小さい．同一デバイスにおいて DPR システムの消費電力が削減された要因として，7.2 節で述べたように，待機中ロジックが削減されクロックの供給面

表 11　Camellia + MISTY1 + TDEA の暗号化時の消費電力
Table 11　Power consumption of the non-PR circuit with Camellia, TDEA and MISTY1.

	Thr'put	Camellia + MISTY1 + TDEA			PR-Crypt	
	[Mbps]	静的 [mW]	動的 [mW]	合計 [mW]	合計 [mW]	削減率 (%)
待機時	-	23.157	29.178	52.30035		
Camellia	109.7	23.157	233.382	256.539	228.892	(10.8)
MISTY1	118.2	23.157	388.9515	412.1085	420.436	(−2.02)
TDEA	28.98	23.157	53.406	76.563	60.161	(21.4)

(XC2VP7，24 MHz)

積が小さくなったことがあげられる．

ここで，7.2.1 項と同様に TDEA の実行時電力について考える．PR-Crypt が SEED から TDEA に切り替えられたとすると，式 (13) に表 10 の結果を適用することで，

$$t_r > \frac{44.392 + 90}{78.1761 - 60.161} \cdot 628.89 = 4691.5 \tag{23}$$

となる．ゆえに，TDEA による暗号化処理が約 4.7 秒以上連続する場合に，PR-Crypt の消費電力量は Camellia+SEED+TDEA の非 DPR 回路を下回る．

また，同じ回路で TDEA の待機電力について考える．式 (21) より，

$$t_r > \frac{44.394 + 90}{52.8047 - 32.910} \cdot 628.89 = 4248.3 \tag{24}$$

となるため，待機時間が約 4.2 秒以上連続する場合は PR-Crypt の消費電力量は非 DPR 回路を下回ることが分かる．

しかし，MISTY1 の消費電力は PR-Crypt の方が大きいという結果が得られた．MISTY1 は，表 7 における省電力効果が最も小さかったモジュールである．この理由として，PR-Crypt では MISTY1 単体の消費電力が比較的大きくなっていることが考えられる．PR-Crypt では，PRR という限られた領域にモジュールを実装するため，非 DPR 回路と比べて配置配線の結果が大きく異なることが考えられ，これが消費電力に影響を与えた可能性がある．配置配線の結果がどのように消費電力に影響するか解明することは，今後の課題である．

7.4　ASIC との比較

NonPR-Crypt では DPR を使用していないため，これと同等の機能を持つ回路は ASIC でも実現可能である．暗号モジュールを ASIC で実装した場合，消費電力は**表 12** のようになる．使用したセルライブラリは VDEC より提供される Hitachi の 0.18 μm 京大版であり，回路の論理合成には Synopsys 社の Design Compiler を使用した[⋆1]．表 12 は暗号モジュールのコアのみの消費電力であり，周辺回路の消費電力は含まれていない．

表 12　ASIC に実装時の暗号モジュールの消費電力
Table 12　Power consumption of the cryptographic hardware implemented on an ASIC.

	速度重視		面積重視	
暗号モジュール	[Mbps]	[mW]	[Mbps]	[mW]
AES	1841.73	53.46	846.56	6.23
Camellia	884.77	64.46	400.09	5.87
SEED	684.35	121.72	268.28	9.77
TDEA	448.93	53.80	153.26	4.47
MISTY1	716.85	60.14	202.71	2.70

表 12 が示すように，すべての暗号モジュールについて，PR-Crypt の消費電力は ASIC 実装時を上回ることが分かる．消費電力の差は，速度重視の TDEA との比較における 6.36 mW が最小で，面積重視の SEED との比較における 504 mW が最大である．しかし，FPGA は初期開発費用が低く，生産量が少ない場合には ASIC よりもコスト的に有利である．また，FPGA は開発期間が短いため，市場の要求に即座に対応できるメリットがある．ゆえに，FPGA を使用することによる消費電力の増分がシステム全体の消費電力に対して小さい場合は，コストや市場への即応性を優先して FPGA を使用するケースがあり，DPR によって FPGA の消費電力を抑える手法は実用面においても有効である．

7.5　部分再構成時電力

表 8 より，DPR の消費電力はビットストリームのサイズのみに依存するわけではないことが分かる．たとえば AES が実装されている状態で AES のビットストリームを構築する場合のように，実際には PRM が変化しない DPR を行うと，異なるモジュールを構築する場合よりも消費電力は低くなることが分かる．これは，FPGA 内のコンフィギュレーションメモリの値の変化量（ハミング距離）が，DPR 時の消費電力に大きく影響すると考えられる．ゆえに DPR 回路においては，論理合成や配置配線において，回路規模や遅延だけでなく，DPR 前後のコンフィギュレーションメモリのハミング距離を最小化するような最適化戦略が有効であると考えられる．

また表 8 より，DPR 時の消費電力が構築される PRM によって大きく変わることが分かる．ゆえに，DPR 時の消費電力を観測することによって，どの PRM が構築されているかを特定できる可能性がある．ビットストリームが通信経路上で暗号化されていても，FPGA

⋆1 東北大学青木研究室の協力による．

内で復号されてから DPR が行われるため，消費電力を測定することで平文ビットストリームを特定できる可能性がある．たとえば，暗号回路をランダムな時間間隔で切り替えることで実行中のアルゴリズムを特定できないようにするセキュリティ対策が考えられるが，そのような対策において新たな問題となりうる．

このような解析を行うためには，PRM のビットストリームを自由に入手・再構成することができるという前提が必要であるため，悪意のある第三者が解析を実行することは難しい．しかし，セキュリティの観点から，DPR 時の消費電力の差を隠蔽する必要がないとはいえない．この点については，引き続き研究を行う．

8. おわりに

アプリケーション切替え型 DPR システムは回路の小型化に有効であるが，DPR に固有のオーバヘッドによる動的な電力消費があり，また動作しているロジックの面積自体は非 DPR システムとそれほど変わらないため，動的消費電力の削減効果はこれまで不明であった．そこで本稿では，ISO/IEC 18033-3 標準の 5 つの暗号アルゴリズムをアプリケーションとして切り替える DPR システムを Xilinx FPGA 上に実装し，回路規模と消費電力の性能評価を行った．

その結果このマルチ暗号システムにおいて DPR は非 DPR に対して，消費電力は実行時に最大 40%，待機時に最大 53%削減という大きな効果が示された．部分再構成を頻繁に行ってアルゴリズムを切り替えるような特殊な状況下でなければ，DPR による消費電力のオーバヘッドが抑えられるため，システム全体で高い消費電力の削減が期待できる．もちろん，高い省電力効果を得るためには，アプリケーションが頻繁に切り替わらないようなシステムアーキテクチャを構成することも重要である．また静的消費電力は全体の回路規模に比例するため，待機時間が長い用途において特に DPR は大きな省電力効果を発揮することができる．DPA によるマルチ暗号システムの例では，回路規模が非 DPR システムの約 1/3 に削減され，使用するデバイスを XC2VP30 から XC2VP7 へと小さくすることができた．このように，アプリケーション切替え型の DPR 方式の利用は，消費電力の削減だけでなく，システムの小型軽量化と低価格化にも有効である．今後は，さらなる低消費電力化を目的に，DPR 時の消費電力を低減させるための手法の開発と，PRM の配置配線結果が消費電力に与える影響について研究を進めていきたい．また DPR 時の回路データのエラーや，悪意のある第三者によるシステムの不当な改ざんを防ぐための，DPR のセキュリティ対策についても報告していく予定である．

謝辞　本研究を行うにあたり，SASEBO の使用方法を指導していただいた産業技術総合研究所情報セキュリティ研究センターの佐藤証氏に深謝する．また，ASIC の消費電力データを提供していただいた東北大学青木研究室の菅原健氏をはじめ同研究室のメンバに深謝する．本研究は，平成 19 年度総務省戦略的情報通信研究開発推進制度（SCOPE）の委託研究「超高速ネットワークに対応した悪意ある通信の遮断技術の研究開発」（課題番号：072003008）の成果である．

参 考 文 献

1) Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T.: Specification of Camellia — A 128-bit Block Cipher Version 2.0 (2001).
2) Atmel Corporation: FPSLIC on-chip Partial Reconfiguration of the Embedded AT40K FPGA (2002).
3) Cryptographic Hardware Project: http://www.aoki.ecei.tohoku.ac.jp/crypto/, Aoki Lab., Tohoku University.
4) 堀　洋平，坂根広史，戸田賢二：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，信学技報 RECONF2007-56，pp.31–36 (2008).
5) ISO/IEC 18033-3: Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers (2005).
6) Jackson, B.: *Partial Reconfiguration Design with PlanAhead 9.2*, Xilinx, Inc. (2007).
7) KISA: SEED Algorithm Specification.
8) Lorenz, M.G., Mengibar, L., Valderas, M.G. and Luis, E.: Power Consumption Reduction Through Dynamic Reconfiguration, *FPL'04*, pp.751–760 (2004).
9) Matsui, M.: Specification of MISTY1 — A 64-bit Block Cipher. NESSIE Project.
10) National Institute of Standards and Technology: *Announcing the Advanced Encryption Standard* (*AES*), FIPS PUB. 197 (2001).
11) National Institute of Standards and Technology: The Advanced Encryption Standard Algorithm Validation Suite (DES) (2002).
12) National Institute of Standards and Technology: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (2004).
13) Noguera, J. and Kennedy, I.O.: Power Reduction in Network Equipment through Adaptive Partial Reconfiguration, *FPL'07*, pp.240–245 (2007).
14) Side-channel Attack Standard Evaluation Board (SASEBO). http://www.rcis.aist.go.jp/special/SASEBO/. Research Center for Information Security, National Institute of Advanced Industrial Science and Technology.
15) Sugawara, T., Homma, N., Aoki, T. and Satoh, A.: ASIC Performance Comparison

for the ISO Standard Block Ciphers, *JWIS 2007*, pp.485–498 (2007).
16) TOSHIBA: TC58FVT004/B004FT-85,-10,-12 (1998).
17) U.S. Department of Commerce/National Institute of Standards and Technology: *Data Encryption Standard* (*DES*), FIPS PUB. 46-3 edition (1999).
18) Xilinx: Two Flows for Partial Reconfiguration: Module Based or Difference Based (2004).
19) Xilinx: *Development System Reference Guide*, for ISE8.1i edition (2005).
20) Xilinx, Inc.: *Early Access Partial Reconfiguration User Guide For ISE 8.1.01i* (2006).
21) Xilinx, Inc.: *Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet v4.6* (2007).

(平成 20 年 1 月 29 日受付)
(平成 20 年 5 月 2 日採録)

堀　洋平（正会員）

1999 年筑波大学第三学群工学システム学類卒業．2004 年同大学院博士課程修了．同年（独）産業技術総合研究所情報処理研究部門（現，情報技術研究部門）特別研究員．多目的映像表示装置，コンテンツ保護システム等の研究開発を行う．現在，FPGA の動的部分再構成を利用したリコンフィギャラブルシステム，暗号ハードウェアモジュールの耐タンパ性評価に関する研究に従事．電子情報通信学会会員．博士（工学）．

坂根　広史（正会員）

1990 年山口大学工学部電子工学科卒業．1992 年電気通信大学大学院電気通信学研究科博士前期課程電子工学専攻修了．同年通商産業省工業技術院電子技術総合研究所入所．2001 年独立行政法人産業技術総合研究所に組織変更．現在，同所主任研究員．同年電気通信大学大学院情報システム学研究科博士後期課程情報ネットワーク学専攻修了．博士（工学）．2002 年より 2005 年までデラウェア大学客員研究員．マルチコアアーキテクチャおよびそのエミュレーション方式，情報セキュリティを含む FPGA 応用，および暗号実装の安全性に関する研究に従事．電子情報通信学会会員．

片下　敏宏

2006 年筑波大学大学院システム情報工学研究科卒業．博士（工学）．現在，産業技術総合研究所情報技術研究部門特別研究員．主としてネットワークセキュリティ，回路設計に関する研究に従事．電子情報通信学会会員．

戸田　賢二（正会員）

1982 年慶應義塾大学工学研究科修士課程終了．同年電子技術総合研究所入所．以来，並列コンピュータのアーキテクチャの研究に従事し，記号処理用データ駆動計算機や実時間処理用並列計算機の開発を行った．近年は組込応用をターゲットとし，開発環境の整備と共に実時間処理用ハードウェアやネットワークの実用化研究を推進中．