2011 情財第 399 号

情報セキュリティ対策基盤整備事業

「電子政府推奨暗号の実装」

評価報告書

平成 24 年 12 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

［改訂履歴］

日付	改訂内容
2012 年 12 月 11 日	評価報告書初版発行
2012 年 12 月 21 日	「2. 評価結果」内のデータを修正（表 1-1、表 1-2、表 2-1、表 2-2、表 3-1、表 3-2、表 4-1、表 4-2、表 5-1、表 5-2、表 6-1、表 6-2）

目次

1. 評価条件

各暗号回路の規模および処理性能評価は，Xilinx 社の Virtex-5 だけでなく，Virtex-6，Spartan-3，Spartan-6，さらに ALTERA 社の Cyclone III，Stratix III などの主要 FPGA に対する網羅的な評価を行った．Xilinx 社 FPGA の論理合成には ISE WebPACK Release 12.4 を，ALTARA 社の論理合成には Quartus II Version 9.0 を用い，論理合成オプションはデフォルトの値を用いた．

具体的な評価項目は下記の通りである．ここで回路効率は，小型実装，高速実装に適しているアルゴリズムだけでなく回路規模と速度のバランスに優れたアルゴリズムを調べるのに重要な指標となる．なお，本業務では，「処理速度」および「リソース量」の評価が求められているが，これに加えて参考情報として Xilinx 社の FPGA に対しては「消費電力」の評価も行った．

- 処理速度
  クリティカルパス遅延，最大動作周波数，クロック数，スループット
  鍵スケジュールのクロック数（ブロック暗号の場合）
  IV セットアップと鍵セットアップクロック数（ストリーム暗号の場合）
- リソース量
  LUT 数，FF 数，LUT+FF ペア数
- 回路効率
  処理速度/リソース量
- 消費電力
  24MHz 動作時の消費電力

さらに，設計した回路の動作テストは，各アルゴリズム仕様書のテストベクタを用いて，シミュレーションおよび SASEBO-GII 上による実機での確認を行った．スループットは SASEBO-GII のインタフェースによるオーバーヘッドや，24MHz というシステムクロックで律速されてしまう．そこで，インタフェース回路を除いた暗号コアの単体の性能として，ECB モードにおいて最短サイクルでデータを入力し，最大動作周波数（CAD レポートによる）で処理した場合のスループットを求めた．なお，ECB モードはデータパスのパイプライン化によりスループットを大幅に向上させることができるが，各種暗号利用モードに対応できないため，パイプライン処理での実装および評価は行わないものとした．

暗号回路マクロの入出力には暗号文，平文，鍵等のデータバスがそのままのビット幅で出ているため，インタフェース回路を通さないと FPGA の I/O ピンが不足し各デバイスに実装することができなかった．そこで，回路規模と動作速度の評価は，配置配線前の暗号回路マクロ単体の論理合成結果を用いた．Xilinx 社の FPGA に対しては消費電力評価を行っているが，各デバイスへ配置配線する必要があるため，インタフェース回路を含めて評価している．

図 1~5 に，Xilinx 社の Virtex-5/-6，Spartan-3，Spartan-6，そして ALTERA 社の Cyclone III，Stratix III の基本ロジックセルを簡略化した構成を示す．FPGA の基本セルは，汎用論理ゲートである LUT(Look-Up Table)，キャリーロジック，1 ビットの FF(Flip-Flop)その他制御用のセレクタ等から構成される．Xilinx 社の FPGA の基本ロジックセルはいずれも Slice と呼ばれるが，FPGA の種類によっ

てその構成が異なる. 図 1 の Virtex-5/-6 は 6 入力 2 出力 LUT, キャリーロジック, 1 ビットの FF(Flip-Flop)のセットを 4 つ有している. また, 図 2 の Spartan-6 も同様の構成をしているが, 一つの LUT に対して 2 ビット分の FF が割り当てられる点が異なる. 図 3 の Spartan-3 の Slice は 4 入力 1 出力の LUT と FF のセットが 2 つ入っている. また, この LUT と FF のセットを 2 つ合わせたものは CLB(Configurable Logic Block)と呼ばれる. Xilinx 社の FPGA の回路規模を示す値として, Slice が用いられることが多いが, 上記のように規模がシリーズによって異なるので, 今回は, 1 つの LUT と FF のセット(後出の表では LUT+FF pair と表記)を基本単位とした. つまり, Virtex-5/-6 では Slice の 1/4, Spartan-3 では Slice の 1/2 が基本単位の LUT+FF pair となる. なお Spartan-6 は FF が多いので, Slice の 1/4 にあたる 1 つの LUT と 2 ビット分の FF を基本単位 pair とている. ところで, この基本単位の pair の全てで LUT と FF が使われるわけではなく, どちらか一方しか利用されないものが多く存在する. そこで, FPGA 全体で使用された LUT 数と FF の数も別途示した.

ALTERA 社の FPGA の基本セルは従来, 図 4 の Cyclone III に示した LE(Logic Element)であった. これは, 4 入力 1 出力の LUT, キャリーロジック, 1 ビットの FF から構成されている. しかし, 図 5 の Stratix III はこれとは異なる ALM (Adaptive Logic Module)を基本セルとしている. それは, 8 入力 2 出力の LUT 一つに対して, 2 つのキャリーロジックと 2 ビット分の FF がセットとなっている. しかしながら, この LUT は 2 つの 4 入力 1 出力 LUT として利用可能なため, この 1/2 サイズの LUT と 1 ビット分 FF のペア(ALM の 1/2)を基本単位としてとし評価することにした. 後出の表 6-2 の Stratix III の LUT はこの 4 入力 1 出力 LUT で換算した値を示している.

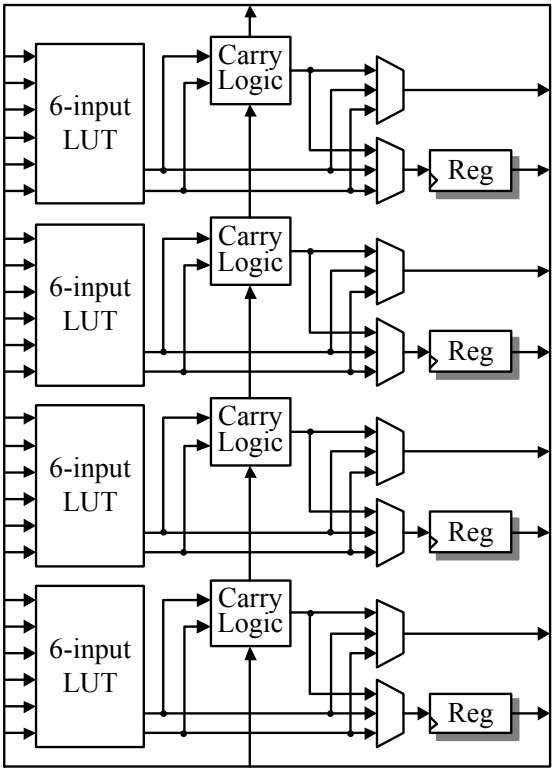

図 1 Virtex-5/-6 の基本セル Slice の構造

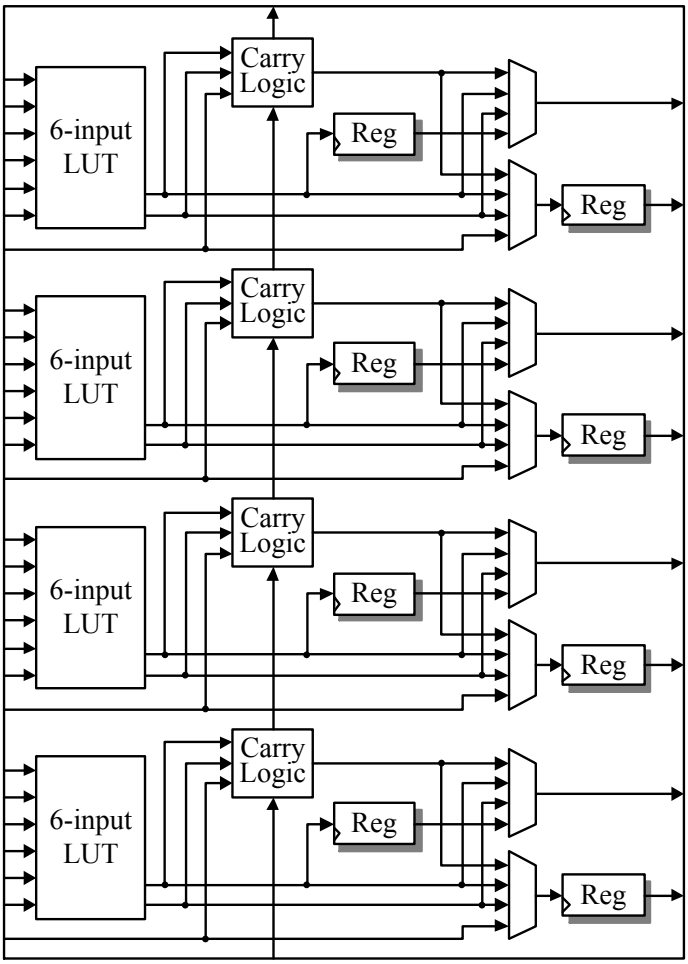

図 2　Spartan-6 の基本セル Slice の構造

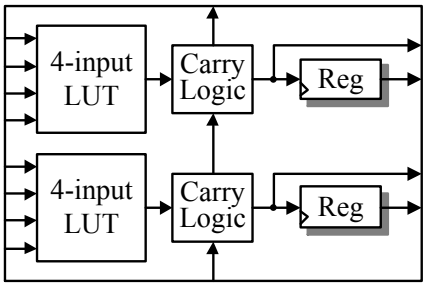

図 3　Spartan-3 の基本セル Slice の構造

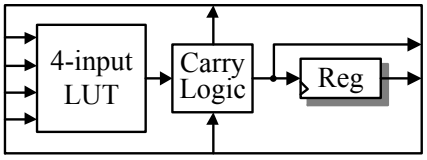

図 4　Cyclone III の基本セル LE の構造

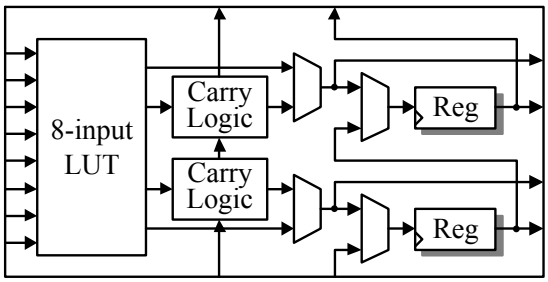

図 5　Stratix III の基本セル ALM の構造

2. 評価結果

表 1-1~6.2 に，各 FPGA デバイス上での各暗号回路の論理合成結果を示す．Spartan-3 では MULTI-S01 がリソース不足のため入りきらなかったが，論理合成結果にリソース使用量 100%以上として回路規模と動作速度が示されるので，表 3-2 にはこれを記入している．また，インタフェース回路を付加すると MULTI-S01 と Hierocrypt-3 は Spartan-3 に入りきらず，消費電力評価ができなかったため，表 3-3 で空欄となっている．消費電力は，静的消費電力と動的消費電力に分けられるが，24MHzと低速動作で評価しているため，静的消費電力の割合が非常に高い．またそれはアルゴリズムに関係なくデバイスで決まる一定の値である．動的消費電力は，クロック，ロジック，信号線，I/O に分けて記載している．グローバル配線として FPGA 全体を走るクロック線は寄生容量が大きいため，これもまた大きな消費電力を必要とする．一方ほとんど動いていないI/Oの消費電力は無視できるほど小さい．したがって，ロジックのスイッチングと信号線の充放電にかかる消費電力をある程度の評価尺度として利用することができる．しかしながら，この消費電力評価は，テストベクタを用いたシミュレーションによる信号遷移ではなく，論理合成ツールのデフォルトの遷移確率（FF:12.5%，I/O:12.5%）に基づいている．また，CIPHERUNICORN-A は 24MHz で動作しないが，最大遅延パスは考慮せずに，各ロジックが仮定した遷移確率で個別に 24MHz スイッチングしたときの電力評価を行っていると考えられる．また，フォールスループが存在する場合，そのパスは電力評価から削除される．このような理由から，表に示した消費電力は，あくまで参考程度ととらえるべきものである．

回路規模の評価においては，ブロック暗号では AES と Camellia がいずれのデバイスにおいても優れた値を示している．AES は動作周波数が高く，暗号化・復号のサイクル数も 11 と少ないため，スループットもブロック暗号中で最も高い．その結果，回路効率を示す単位回路あたりのスループット kbps/pair はいずれのデバイスにおいても Camellia の 2 倍前後となっている．

Hierocrypt-3 も AES と同様の SPN 構造を持つブロック暗号であるが，著しく低い性能となった．これはメインターゲットした Virtex-5（Xc5lxff324-3）の制約によるところが大きい．アルゴリズムと回路データパスの詳細は 5.5 節に記したが，128 ビットの SPN 型ブロック暗号の Hierocryt-3 のデータパスは128ビットで組むことが回路規模と速度のバランスからは最も好ましい．しかしながら，32ビット入出力の MDS_L, $iMDS_LL$ 関数は 1 組で Virtex-5 の 30%のリソース必要とし，4 組実装できないため，1 組を 4 回繰り返して利用することとした．さらに，この関数ブロックがクリティカルパスとなり，ターゲットの 24MHz で動作させることができず，4 クロックに分けて処理を行った．このようなオーバーヘッドによりクロック数が増大し，スループットが大幅に低下してしまっている．したがって，より大きなデバイスをターゲットにデータパスの最適化を行えば，性能を大幅な向上させることが可能である．今回は単純実装でかつ S-box もテーブル実装を基本としているため，暗号化と復号でコンポーネントが独立しているが，それらを共有化することで回路規模の大幅な削減も可能であると考えられる．

全アルゴリズムの中では，疑似乱数生成器 MUGI の回路性能が非常に高い．AES の暗号化のコンポーネントを用い，64 ビット乱数を 2 クロックで出力できるという点が AES の 6 倍前後という高いスループットを実現している理由である．今回はインタフェースの制限で2クロックのサイクルとなっているが，MUGI に特化したインタフェース回路を設計すれば， 64 ビット疑似乱数を毎クロック出力して

スループットをさらに 2 倍とすることも可能である. 非常にシンプルな構造のため回路規模は AES の 6 割程度となっている. しかし, 疑似乱数生成器は内部ステート保持のために多数の FF レジスタが使用されていることに注意が必要である. 先に述べたように, FPGA の基本セルは, 論理ゲートの LUT と FF がペアになっており, 表からブロック暗号は FF を使用していない基本セルが多数存在することがわかる. ASIC 実装の場合, 大きなゲート数を必要とする無駄な FF を省くことができるので, MUGI の半分の FF しか必要としない AES や Camellia のほうが小さな回路となると考えられる.

ここで示した回路実装性能は, Virtex-5 を実装した SASEBO-GII ボードでの 24MHz 動作を前提に, シンプルなデータパスによる設計を行っている. したがって, ここに示した値が各暗号アルゴリズムの絶対的な回路性能を示すものではなく, 実装するデバイスや求められる回路規模や動作速度などの様々な制約に応じた最適化により, 大きく異なる性能が示される可能性に留意する必要がある.

表 1-1 Virtex-5 (xc5lvlx50-1ff324) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	スループット (Mbps)
AES	128	11	11	7.331	136.402	1,587.22
Camellia	128	5	23	6.982	143.225	797.08
CIPHERUNICORN-A	128	40	17	45.933	21.771	163.92
Hierocrypt-3	128	886	488	34.873	28.676	7.52
SC2000	128	17	15	9.961	100.392	856.68
MULTI-S01	64	39	5	8.197	121.996	1,561.55
MUGI	64	16	2	3.109	321.596	10,291.07

表 1-2 Virtex-5 (xc5lvlx50-1ff324) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/pair)
	LUT-FF pair	LUT	FF	
AES	2,645	2,385	529	600.08
Camellia	2,361	2,340	547	337.60
CIPHERUNICORN-A	8,707	6,629	2,593	18.83
Hierocrypt-3	13,457	10,517	4,660	0.56
SC2000	9,347	9,238	660	91.65
MULTI-S01	18,102	17,987	10,039	86.26
MUGI	2,087	2,086	1,231	4,931.04

表 1-3 Virtex-5 (xc5lvlx50-1ff324) 上の消費電力

アルゴリズム	消費電力 (mW)						
		静的消費電力	動的消費電力				
				クロック	ロジック	信号線	I/O
AES	430.54	416.77	13.77	10.68	0.91	2.10	0.08
Camellia	431.64	416.78	14.86	13.15	0.37	1.26	0.08
CIPHERUNICORN-A	532.82	417.96	114.86	34.12	17.33	63.34	0.08
Hierocrypt-3	462.45	417.14	45.31	44.66	0.16	0.41	0.08
SC2000	436.72	416.84	19.88	19.52	0.01	0.27	0.08
MULTI-S01	485.15	417.40	67.75	67.00	0.08	0.59	0.08
MUGI	431.48	416.78	14.71	14.43	0.01	0.18	0.08

表 2-1　Virtex-6 (xc6vlx75t-3ff484) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	ｽﾙｰﾌﾟｯﾄ (Mbps)
AES	128	11	11	4.361	229.317	2,668.42
Camellia	128	5	23	4.353	229.737	1,278.54
CIPHERUNICORN-A	128	40	17	25.993	38.472	289.67
Hierocrypt-3	128	886	488	21.194	47.184	12.38
SC2000	128	17	15	5.708	175.190	1,494.95
MULTI-S01	64	39	5	5.331	187.582	2,401.05
MUGI	64	16	2	1.823	548.463	17,550.82

表 2-2　Virtex-6 (xc6vlx75t-3ff484) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/pair)
	LUT-FF pair	LUT	FF	
AES	2,624	2,368	525	1,016.93
Camellia	2,272	2,268	541	562.74
CIPHERUNICORN-A	8,564	6,520	2,582	33.82
Hierocrypt-3	13,290	11,019	4,638	0.93
SC2000	7,040	6,935	660	212.35
MULTI-S01	18,025	17,976	10,038	133.21
MUGI	1,515	1,512	1,229	11,584.70

表 2-3　Virtex-6 (xc6vlx75t-3ff484) 上の消費電力

アルゴリズム	消費電力 (mW)						
		静的消費電力	動的消費電力				
				クロック	ロジック	信号線	I/O
AES	1,014.80	1,007.50	7.30	1.30	2.73	3.08	0.19
Camellia	1,010.87	1,007.41	3.46	1.60	0.67	0.99	0.19
CIPHERUNICORN-A	1,063.87	1,008.64	55.23	2.87	21.12	31.05	0.19
Hierocrypt-3	1,013.44	1,007.47	5.97	5.65	0.01	0.12	0.19
SC2000	1,010.16	1,007.39	2.77	2.46	0.01	0.11	0.19
MULTI-S01	1,019.89	1,010.12	9.77	6.70	1.11	1.52	0.44
MUGI	1,012.45	1,007.45	5.00	3.09	1.02	0.69	0.19

表 3-1　Spartan-3 (xc3s1400an-5fgg676) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	ｽﾙｰﾌﾟｯﾄ (Mbps)
AES	128	11	11	12.055	82.950	965.24
Camellia	128	5	23	13.158	76.002	422.97
CIPHERUNICORN-A	128	40	17	79.433	12.589	94.79
Hierocrypt-3	128	886	488	67.727	14.765	3.87
SC2000	128	17	15	16.093	62.139	530.25
MULTI-S01	64	39	5	19.378	51.605	660.54
MUGI	64	16	2	5.935	168.482	5,391.42

表 3-2 Spartan-3 (xc3s1400an-5fgg676) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/spair)
	LUT-FF pair	ロジック (LUT)	レジスタ (FF)	
AES	2,827	5,585	527	341.43
Camellia	2,548	4,963	539	166.00
CIPHERUNICORN-A	9,946	17,612	2,607	9.53
Hierocrypt-3	10,216	18,863	4,686	0.38
SC2000	6,596	12,334	695	80.39
MULTI-S01*1	16,758	31,575	10,091	39.42
MUGI	1,913	3,683	1,237	2,818.31

*1 リソース不足のため Spartan-3 にマップできず.

表 3-3 Spartan-3 (xc3s1400an-5fgg676) 上の消費電力

アルゴリズム	消費電力 (mW)						
		静的消費電力	動的消費電力				
				クロック	ロジック	信号線	I/O
AES	83.87	63.21	20.66	12.95	1.59	4.06	2.07
Camellia	97.53	63.32	34.21	16.91	4.25	10.35	2.70
CIPHERUNICORN-A	263.50	64.67	198.83	22.95	36.70	138.08	1.10
Hierocrypt-3*2	-	-	-	-	-	-	-
SC2000	118.22	63.48	54.74	20.96	10.83	21.84	1.10
MULTI-S01*2	-	-	-	-	-	-	-
MUGI	108.22	63.40	79.19	20.52	4.77	18.46	1.07

*2 リソース不足のため Spartan-3 にマップできず.

表 4-1 Spartan-6 (xc6slx45-3ffg676) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	スループット (Mbps)
AES	128	11	11	9.739	102.679	1,194.81
Camellia	128	5	23	8.515	117.446	653.61
CIPHERUNICORN-A	128	40	17	55.374	18.059	135.97
Hierocrypt-3	128	886	488	47.102	21.231	5.57
SC2000	128	17	15	12.080	82.782	706.41
MULTI-S01	64	39	5	13.221	75.640	968.19
MUGI	64	16	2	4.340	230.434	7,373.89

表 4-2 Spartan-6 (xc6slx45-3ffg676) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/pair)
	LUT-FF pair	ロジック (LUT)	レジスタ (FF)	
AES	2,619	2,365	525	456.21
Camellia	2,427	2,407	562	269.31
CIPHERUNICORN-A	8,571	6,532	2,585	15.86
Hierocrypt-3	14,091	11,799	4,654	0.40
SC2000	7,189	7,031	678	98.26
MULTI-S01*1	18,018	17,928	10,027	53.73
MUGI	1,548	1,539	1,238	4,763.49

表 4-3　Spartan-6 (xc6slx45-3ffg676) 上の消費電力

アルゴリズム	消費電力 (mW)						
		静的消費電力	動的消費電力				
				クロック	ロジック	信号線	I/O
AES	35.34	30.98	4.36	0.07	1.75	1.16	1.37
Camellia	32.85	30.95	2.75	1.70	0.12	0.01	0.07
CIPHERUNICORN-A	130.17	32.33	97.84	2.98	25.59	69.20	0.07
Hierocrypt-3[*2]	38.81	31.03	8.78	6.55	0.26	0.91	0.07
SC2000	34.19	30.97	3.22	2.88	0.06	0.21	0.07
MULTI-S01[*2]	55.38	38.76	16.62	8.20	3.17	4.92	0.32
MUGI	43.51	38.60	4.61	2.87	1.26	0.71	0.07

表 5-1　Cyclone III (EP3C40F484C6) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	ｽﾙｰﾌﾟｯﾄ (Mbps)
AES	128	11	11	13.205	75.73	881.22
Camellia	128	5	23	12.581	79.49	442.38
CIPHERUNICORN-A	128	40	17	88.184	11.34	85.38
Hierocrypt-3	128	886	488	46.297	21.60	5.67
SC2000	128	17	15	16.104	62.10	529.92
MULTI-S01	64	39	5	27.541	36.31	464.77
MUGI	64	16	2	4.331	230.89	7,388.48

表 5-2　Cyclone III (EP3C40F484C6) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/pair)
	LUT-FF pair	LUT	FF	
AES	6,614	6,358	526	133.24
Camellia	3,544	3,544	540	124.82
CIPHERUNICORN-A	27,096	24,920	2,584	3.15
Hierocrypt-3	22,044	19,431	4,631	0.26
SC2000	15,450	13,402	2,706	34.30
MULTI-S01	27,601	27,473	10,027	16.84
MUGI	2,458	2,453	1,230	3,005.89

表 6-1　Stratix III (EP3SE50F484C2) 上の処理速度

アルゴリズム	ブロック長 (bit)	鍵設定 (clock)	サイクル数 (clock)	遅延時間 (ns)	動作周波数 (MHz)	ｽﾙｰﾌﾟｯﾄ (Mbps)
AES	128	11	11	7.238	138.16	1,607.68
Camellia	128	5	23	6.665	150.04	835.01
CIPHERUNICORN-A	128	40	17	42.644	23.45	176.56
Hierocrypt-3	128	886	488	34.873	28.67	7.52
SC2000	128	17	15	9.887	101.15	863.15
MULTI-S01	64	39	5	11.615	86.10	1,102.08
MUGI	64	16	2	2.690	371.61	11,891.52

表 6-2 Stratix III (EP3SE50F484C2) 上の回路規模

アルゴリズム	回路規模			回路効率 (kbit/pair)
	LUT-FF pair	LUT	FF	
AES	2,701	2,446	526	595.22
Camellia	1,754	1,737	540	476.06
CIPHERUNICORN-A	8,789	6,557	2,584	20.09
Hierocrypt-3	13,654	10,785	4,630	0.55
SC2000	9,768	7,592	2,706	88.36
MULTI-S01	16,688	8,621	10,027	66.04
MUGI	1,405	824	1,230	8,463.72