サイドチャネル攻撃評価用
ISO/IEC 標準暗号 LSI 仕様書

ISO/IEC Standard Cryptographic LSI for Side-channel Attack Evaluation Specification

[第1版]

2008 年 4 月 1 日

（独）産業技術総合研究所
情報セキュリティ研究センター

目次

Page

1. 概要 …… 2
2. 外部仕様 …… 3
    2.1 入出力信号 …… 3
    2.2 コマンド制御 …… 8
3. 内部詳細仕様 …… 12
    3.1 LSI 内部構成 …… 12
    3.2 外部インタフェース …… 15
    3.3 インタフェースレジスタ …… 17
    3.4 クロックツリー …… 21
    3.5 リセット …… 21
    3.6 付帯機能 …… 22
4. LSI の物理レイアウト …… 24

1. 概要

「標準暗号アルゴリズムを実装した専用 LSI」(以下, 暗号 LSI)は, 差分電力解析を始めとする各種実装攻撃の評価を目的に, 公開鍵暗号 RSA および ISO/IEC 18033 (Information technology-Security techniques - Encryption algorithms) Part3:Block ciphers に掲載された全ての共通鍵暗号アルゴリズムを実装したものである. 暗号 LSI は TSMC(Taiwan Semiconductor Manufacturing Company)社の 0.13μm CMOS プロセスを用いて製造し, 160 ピンセラミック QFP パッケージで封止している.

実装したアルゴリズムは下記の 7 種で, AES については異なる 7 種類の実装を行っているため, 計 12 種類の暗号コアの搭載となった. なお, AES の実装⑥と⑦は論理合成をカスタムで行っている. 国内での評価実験用の LSI に加えて海外で使用するために鍵長を制限した LSI の 2 つも設計・製造した. 制限版は DES 以外のブロック暗号の秘密鍵 128bit の上位 72 ビットを固定し, 56bit のみユーザが指定できるようにしており, RSA 暗号は 512bit 鍵だけをサポートしている.

- AES(鍵長:128bit)
  - ① S-Box 実装→合成体, 暗号化/復号サポート
  - ② S-Box 実装→合成体, 暗号化のみサポート
  - ③ S-Box 実装→case 文記述, 暗号化のみサポート
  - ④ S-Box 実装→AND-XOR 実装(1-Stage), 暗号化のみサポート
  - ⑤ S-Box 実装→AND-XOR 実装(3-Stage), 暗号化のみサポート
  - ⑥ ①に擬似 RSL(標準セルライブラリのみで RSL を模擬)を適用した実装
  - ⑦ FPGA 用のネットリストから ASIC 用のネットリストにリターゲットした実装. 元となる RTL ソースは①を用いており, これと同等の論理回路構造を有する.
- DES:暗号化/復号サポート
- MISTY1:暗号化/復号サポート
- Camellia(鍵長:128) 暗号化/復号サポート
- SEED:暗号化/復号サポート
- CAST128:暗号化/復号サポート
- RSA:1024bit のべき乗剰余演算

また, 主な機能は下記のとおりである.

- 暗号アルゴリズムの実行
- 電力情報等サンプリング用のトリガ信号出力機能
- 故障利用攻撃(Fault Injection Attack)時の評価を目的として, 合成体の S-box を用いた暗号化/復号処理機能を有する AES コアにおいて中間値を出力する機能.

2 外部仕様

2.1 入出力信号

表 1 に暗号 LSI の入出力信号の概要を，表 2 および図 1 に 160 ピンのアサイン(Top view)を示す．表 2 の「Signal Name」中の()は将来拡張用であり暗号 LSI では未使用であり，VSS/VDD ピンは「Signal Name」にセル名を記載している．暗号 LSI では，ノイズを減らし暗号アルゴリズム処理の電力や電磁波を精度よく測定するため，LSI 内部と入出力バッファの VDD/VSS を分離する構成とした．

表 1 入出力信号

分類 (総数)	信号名	本数	有意	方向 (LSI 側から)	用途・備考
システム (11)	CLKA	1	--	IN	24MHz クロック入力(制御 FPGA から供給)
	CLKB	1	--	IN	将来の拡張用 ASIC インタフェース回路用クロック. 今回の暗号 LSI では CLK_B は未使用
	HRST_N	1	L	IN	ボード上のリセット回路によって生成されるリセット信号．非同期リセット入力
	LEDO[1:0]	2	L	OUT	LED 駆動用出力(NC ピン)
	SWIN[3:0]	4	--	IN	スイッチ用入力(NC ピン)
	PHIN[1:0]	2	--	IN	ピンヘッダ用入力(NC ピン)
バス制御 (4)	WR_N	1	L	IN	書き込み指示
	RD_N	1	L	IN	読み出し指示
	RSV0	1	--	IN	(NC ピン)
	RSV1	1	--	IN	(NC ピン)
バスアドレス (16)	A[15:0]	16	--	IN	
バスデータ (32)	DI[15:0]	16	--	IN	入力データ
	DO[15:0]	16	--	OUT	出力データ
評価用 (13)	START_N	1	L	OUT	ターゲット処理開始
	END_N	1	L	OUT	ターゲット処理完了
	(TRIG0)	1	--	OUT	(NC ピン)
	(TRIG1)	1	--	OUT	(NC ピン)
	EXEC	1	H	OUT	ターゲット処理中
	STATE[3:0]	4	--	OUT	選択 IP を示す
	MON[3:0]	4	--	OUT	内部モニタ用(詳細未定)
計		76			

表 2 ピンアサイン (1/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
1	PVSS1DGZ					core GND
2	PVSS1DGZ					core GND
3	PVSS2DGZ					I/O GND
4	(SWIN[3])					N.C
5	(SWIN[2])					N.C
6	(SWIN[1])					N.C
7	(SWIN[0])					N.C
8	PVDD2POC					I/O 3.3V
9	(PHIN[1])					N.C
10	(PHIN[0])					N.C
11	N.C					N.C
12	N.C					N.C
13	PVSS2DGZ					I/O GND
14	N.C					N.C
15	N.C					N.C
16	N.C					N.C
17	N.C					N.C
18	N.C					N.C
19	PVDD2DGZ					I/O 3.3V
20	PVDD1DGZ					core 1.2V
21	PVSS1DGZ					core GND
22	PVSS2DGZ					I/O GND
23	N.C					N.C
24	N.C					N.C
25	N.C					N.C
26	(RSV1)					N.C
27	(RSV0)					N.C
28	PVSS2DGZ					I/O GND
29	A[15]	I	3.3V		PDIDGZ	アドレスバス
30	A[14]	I	3.3V		PDIDGZ	アドレスバス
31	A[13]	I	3.3V		PDIDGZ	アドレスバス
32	A[12]	I	3.3V		PDIDGZ	アドレスバス
33	PVDD2DGZ					I/O 3.3V
34	A[11]	I	3.3V		PDIDGZ	アドレスバス
35	A[10]	I	3.3V		PDIDGZ	アドレスバス
36	A[9]	I	3.3V		PDIDGZ	アドレスバス
37	A[8]	I	3.3V		PDIDGZ	アドレスバス
38	PVSS2DGZ					I/O GND
39	PVSS1DGZ					core GND
40	PVSS1DGZ					core GND

表 2 ピンアサイン (2/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
41	PVDD1DGZ					core 1.2V
42	PVDD2DGZ					I/O 3.3V
43	A[7]	I	3.3V		PDIDGZ	アドレスバス
44	A[6]	I	3.3V		PDIDGZ	アドレスバス
45	A[5]	I	3.3V		PDIDGZ	アドレスバス
46	A[4]	I	3.3V		PDIDGZ	アドレスバス
47	PVSS2DGZ					I/O GND
48	PVDD1DGZ					core 1.2V
49	A[3]	I	3.3V		PDIDGZ	アドレスバス
50	A[2]	I	3.3V		PDIDGZ	アドレスバス
51	A[1]	I	3.3V		PDIDGZ	アドレスバス
52	A[0]	I	3.3V		PDIDGZ	アドレスバス
53	PVDD2DGZ					I/O 3.3V
54	PVSS1DGZ					core GND
55	PVSS2DGZ					I/O GND
56	(CLKB)					N.C
57	PVSS2DGZ					I/O GND
58	CLKA	I	3.3V		PDISDGZ	クロック.シュミット
59	PVSS2DGZ					I/O GND
60	PVDD1DGZ					core 1.2V
61	PVSS1DGZ					core GND
62	PVSS2DGZ					I/O GND
63	HRST_N	I	3.3V		PDISDGZ	リセット.シュミット
64	PVSS2DGZ					I/O GND
65	WR_N	I	3.3V		PDIDGZ	書き込み指示
66	RD_N	I	3.3V		PDIDGZ	読み出し指示
67	PVDD2DGZ					I/O 3.3V
68	PVSS1DGZ					core GND
69	DO[15]	O	3.3V	8mA	PDO08CDG	出力データ
70	DO[14]	O	3.3V	8mA	PDO08CDG	出力データ
71	DO[13]	O	3.3V	8mA	PDO08CDG	出力データ
72	DO[12]	O	3.3V	8mA	PDO08CDG	出力データ
73	PVSS2DGZ					I/O GND
74	PVDD1DGZ					core 1.2V
75	DO[11]	O	3.3V	8mA	PDO08CDG	出力データ
76	DO[10]	O	3.3V	8mA	PDO08CDG	出力データ
77	DO[9]	O	3.3V	8mA	PDO08CDG	出力データ
78	DO[8]	O	3.3V	8mA	PDO08CDG	出力データ
79	PVDD2DGZ					I/O 3.3V
80	PVDD1DGZ					core 1.2V

表 2 ピンアサイン (3/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
81	PVSS1DGZ					core GND
82	PVSS1DGZ					core GND
83	PVSS2DGZ					I/O GND
84	DO[7]	O	3.3V	8mA	PDO08CDG	出力データ
85	DO[6]	O	3.3V	8mA	PDO08CDG	出力データ
86	DO[5]	O	3.3V	8mA	PDO08CDG	出力データ
87	DO[4]	O	3.3V	8mA	PDO08CDG	出力データ
88	PVDD2DGZ					I/O 3.3V
89	DO[3]	O	3.3V	8mA	PDO08CDG	出力データ
90	DO[2]	O	3.3V	8mA	PDO08CDG	出力データ
91	DO[1]	O	3.3V	8mA	PDO08CDG	出力データ
92	DO[0]	O	3.3V	8mA	PDO08CDG	出力データ
93	PVSS2DGZ					I/O GND
94	N.C					N.C
95	N.C					N.C
96	N.C					N.C
97	N.C					N.C
98	N.C					N.C
99	PVDD2DGZ					I/O 3.3V
100	PVDD1DGZ					core 1.2V
101	PVSS1DGZ					core GND
102	PVSS2DGZ					I/O GND
103	N.C					N.C
104	N.C					N.C
105	N.C					N.C
106	N.C					N.C
107	N.C					N.C
108	PVSS2DGZ					I/O GND
109	DI[0]	I	3.3V		PDIDGZ	入力データ
110	DI[1]	I	3.3V		PDIDGZ	入力データ
111	DI[2]	I	3.3V		PDIDGZ	入力データ
112	DI[3]	I	3.3V		PDIDGZ	入力データ
113	PVDD2DGZ					I/O 3.3V
114	DI[4]	I	3.3V		PDIDGZ	入力データ
115	DI[5]	I	3.3V		PDIDGZ	入力データ
116	DI[6]	I	3.3V		PDIDGZ	入力データ
117	DI[7]	I	3.3V		PDIDGZ	入力データ
118	PVSS2DGZ					I/O GND
119	PVSS1DGZ					core GND
120	PVSS1DGZ					core GND

表 2 ピンアサイン (4/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
121	PVDD1DGZ					core 1.2V
122	PVDD2DGZ					I/O 3.3V
123	DI[8]	I	3.3V		PDIDGZ	入力データ
124	DI[9]	I	3.3V		PDIDGZ	入力データ
125	DI[10]	I	3.3V		PDIDGZ	入力データ
126	DI[11]	I	3.3V		PDIDGZ	入力データ
127	PVSS2DGZ					I/O GND
128	PVDD1DGZ					core 1.2V
129	DI[12]	I	3.3V		PDIDGZ	入力データ
130	DI[13]	I	3.3V		PDIDGZ	入力データ
131	DI[14]	I	3.3V		PDIDGZ	入力データ
132	DI[15]	I	3.3V		PDIDGZ	入力データ
133	PVDD2DGZ					I/O 3.3V
134	PVSS1DGZ					core GND
135	(LED[0])					N.C
136	(LED[1])					N.C
137	END_N	O	3.3V	8mA	PDO08CDG	暗号処理完了
138	START_N	O	3.3V	8mA	PDO08CDG	暗号処理開始
139	PVSS2DGZ					I/O GND
140	PVDD1DGZ					core 1.2V
141	PVSS1DGZ					core GND
142	PVSS2DGZ					I/O GND
143	STATE[0]	O	3.3V	8mA	PDO08CDG	選択 IP を示す
144	STATE[1]	O	3.3V	8mA	PDO08CDG	選択 IP を示す
145	STATE[2]	O	3.3V	8mA	PDO08CDG	選択 IP を示す
146	STATE[3]	O	3.3V	8mA	PDO08CDG	選択 IP を示す
147	PVDD2DGZ					I/O 3.3V
148	PVSS1DGZ					core GND
149	(MON[0])					N.C
150	(MON[1])					N.C
151	(MON[2])					N.C
152	(MON[3])					N.C
153	PVSS2DGZ					I/O GND
154	PVDD1DGZ					core 1.2V
155	EXEC	O	3.3V	8mA	PDO08CDG	暗号処理中
156	N.C					N.C
157	N.C					N.C
158	N.C					N.C
159	PVDD2DGZ					I/O 3.3V
160	PVDD1DGZ					core 1.2V

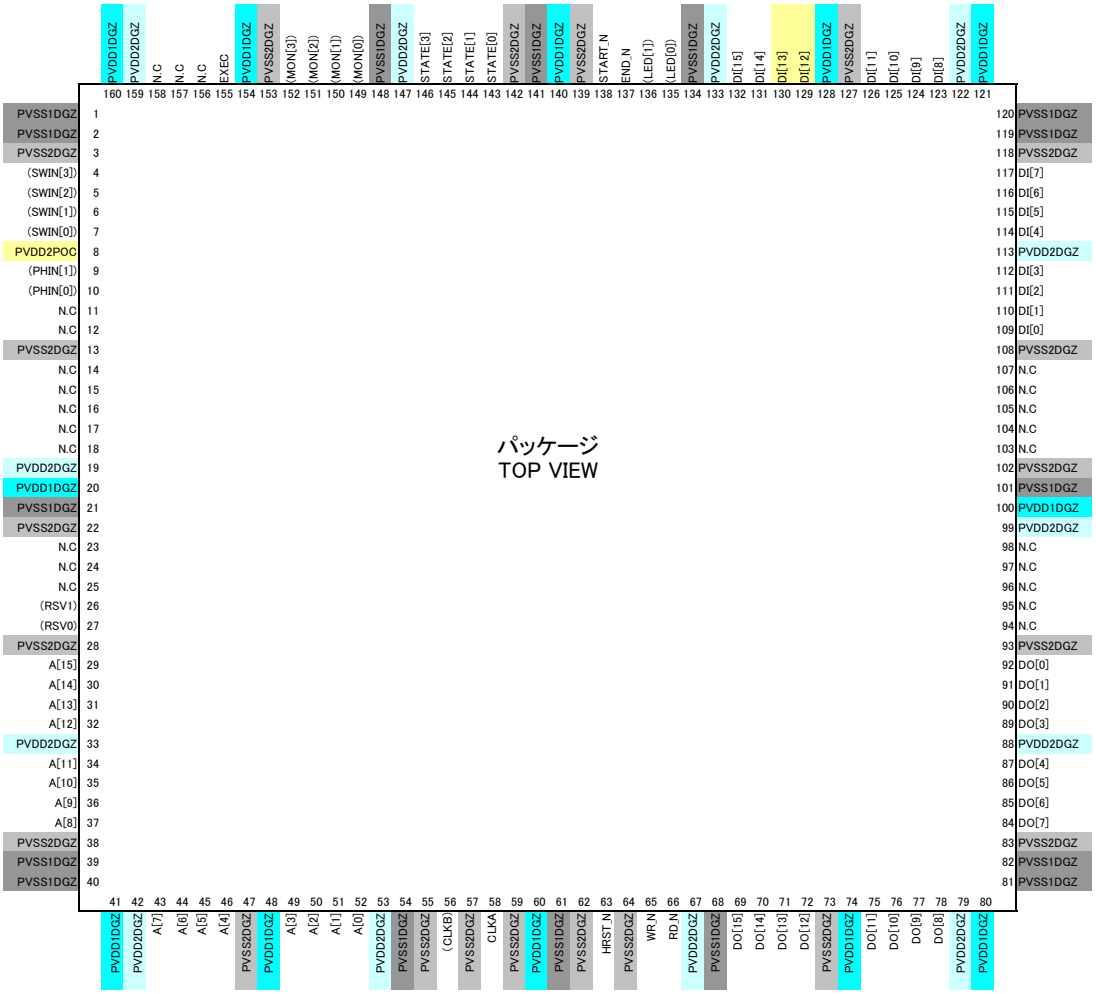


図 1　ピンアサインイメージ

2.2　コマンド制御

暗号 LSI のインタフェースレジスタ，及びアドレスマップ一覧を表 3 に，データのリード/ライトのタイミングを図 2~4 に示す．このインタフェースレジスタを通じて，以下に示した手順で各暗号 IP コアの制御を行う．暗号 IP の種類については次節で解説する．選択 IP を変更する場合は，①～⑥を改めて実行し，また鍵の変更は，②以降を実行する．インタフェースレジスタの詳細は 3.2 節を参照のこと．

① 動作 IP 選択 ： IP 選択レジスタ(IPSEL)の対応ビットをセット．
② 選択 IP リセット ： CONT の IPRST ビットに 1 を書き込んだ後，同ビットに 0 を書き込む．
③ 出力 IP 選択 ： 出力選択レジスタ(OUTSEL)の対応ビットをセット．
④ 動作モード設定 ： モードレジスタ(MODE)を設定する．暗号 IP で AES_comp を選択した場合は，ラウンド選択レジスタ(RSEL)を設定して途中結果を出力するこもが可能である．
⑤ 鍵設定 ：
　⑤-1　共通鍵暗号は鍵レジスタ KEY0~7，公開鍵暗号は指数レジスタ EXP00~3F と法レジスタ MOD00-3F を設定．
　⑤-2　CONT の KSET ビットを 1 にセットした後，同ビットがクリアされるまで待つ．
⑥ 暗号処理 ： (繰り返し)

⑥-1　共通鍵暗号は入力テキストレジスタ ITEXT0~3(64 ビットブロック暗号)または ITEXT0-7(128 ビットブロック暗号), 公開鍵暗号は IDATA00~3F を設定.

⑥-2　CONT[RUN]をセットした後, 同ビットがクリアされるまで待つ.

⑥-3　共通鍵暗号は OTEXT0~3(64 ビットブロック暗号)または OTEXT0~7(128 ビットブロック暗号), 公開鍵暗号は ODATA00~3F から結果を読み出す. 暗号 IP で AES_comp を選択した場合は, ラウンド選択レジスタ RSEL で指定した途中結果レジスタ RDATA0~7 を読み出すことも可能である.

表 3　インタフェースレジスタ (1/2)

分類		ｱﾄﾞﾚｽ	レジスタ名	略称	R/W	機能など
システム制御		0000	(予約)		--	
		0002	コントロールレジスタ	CONT	R/W	処理開始指示(W)/終了通知(R) 鍵生成指示(W)/終了通知(R) 暗号 IP リセット制御(W)
		0004	IP 選択レジスタ	IPSEL	R/W	動作させる暗号 IP を指定(次節参照)
		0006	(予約)			
		0008	出力選択レジスタ	OUTSEL	R/W	データ出力を行う暗号 IP を指定(次節参照)
		000A	(予約)			
		000C	モードレジスタ	MODE	R/W	動作ﾓｰﾄﾞ, 鍵長, 暗復号などを指定
		000E	ラウンド選択レジスタ	RSEL	R/W	中間値保存ラウンﾄﾞ数指定
		0010	テストレジスタ	TEST	R/W	(未定)
		: 00FF	(予約)			
共通鍵暗号	秘密鍵	0100	鍵レジスタ 0	KEY0	W	共通鍵暗号用鍵(最上位 16 ﾋﾞｯﾄ)
		0102	鍵レジスタ 1	KEY1	W	共通鍵暗号用鍵(KEY0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		010E	鍵レジスタ 7	KEY7	W	共通鍵暗号用鍵(最下位 16 ﾋﾞｯﾄ)
		: 013F	(予約)			
	入力テキスト(→ASIC)	0140	入力ﾃｷｽﾄﾚｼﾞｽﾀ 0	ITEXT0	W	入力テキストデータ(最上位 16 ﾋﾞｯﾄ)
		0142	入力ﾃｷｽﾄﾚｼﾞｽﾀ 1	ITEXT1	W	入力テキストデータ(ITEXT0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		014E	入力ﾃｷｽﾄﾚｼﾞｽﾀ 7	ITEXT7	W	
		: 017F	(予約)			
	出力テキスト(←ASIC)	0180	出力ﾃｷｽﾄﾚｼﾞｽﾀ 0	OTEXT0	R	出力テキストデータ(最上位 16 ﾋﾞｯﾄ)
		0182	出力ﾃｷｽﾄﾚｼﾞｽﾀ 1	OTEXT1	R	出力テキストデータ(OTEXT0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		018E	出力ﾃｷｽﾄﾚｼﾞｽﾀ 7	OTEXT7	R	
		: 01BF	(予約)			
	中間値データ(←ASIC)	01C0	中間値レジスタ 0	RDATA0	R	中間値データ(最上位 16 ﾋﾞｯﾄ)
		01C2	中間値レジスタ 1	RDATA1	R	中間値データ(RDATA0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		01CE	中間値レジスタ 7	RDATA7	R	
		: 01FF	(予約)			

表 3　インタフェースレジスタ　(2/2)

分類		ｱﾄﾞﾚｽ	レジスタ名	略称	R/W	機能など
公開鍵暗号	指数	0200	指数レジスタ 0	EXP00	W	指数(最上位 16 ﾋﾞｯﾄ)
		0202	指数レジスタ 1	EXP01	W	指数(EXP00 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		027E	指数レジスタ 63	EXP3F	W	
		: 02FF	(予約)			
	法	0300	法レジスタ 0	MOD00	W	法(最上位 16 ﾋﾞｯﾄ)
		0302	法レジスタ 1	MOD01	W	法(MOD00 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		037E	法レジスタ 63	MOD3F	W	
		: 03FF	(予約)			
	入力データ (→ ASIC)	0400	入力データレジスタ 0	IDATA00	W	入力データ(最上位 16 ﾋﾞｯﾄ)
		0402	入力データレジスタ 1	IDATA01	W	入力データ(IDATA00 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		047E	入力データレジスタ 63	IDATA3F	W	
		: 04FF	(予約)			
	出力データ (← ASIC)	0500	出力データレジスタ 0	ODATA00	R	出力データ(最上位 16 ﾋﾞｯﾄ)
		0502	出力データレジスタ 1	ODATA01	R	出力データ(ODATA00 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		057E	出力データレジスタ 63	ODATA3F	R	
		: 05FF	(予約)			
(空き)		: FFEF				
LSI 情報 (0xFFF0 ～0xFFFF)		FFF0 :	(予約)			
		FFFC	バージョンレジスタ	VER	R	
		FFFE	(予約)		--	

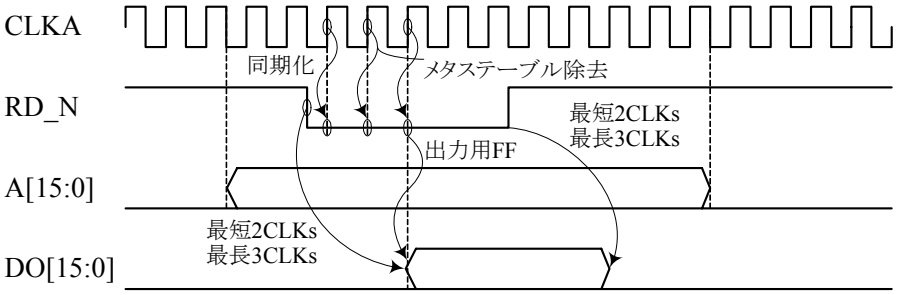


図 2　リードサイクルのタイミングチャート

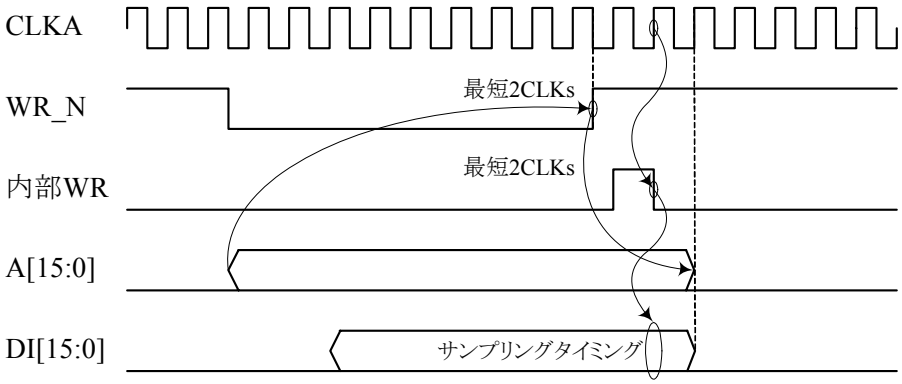


図 3　ライトサイクルのタイミングチャート

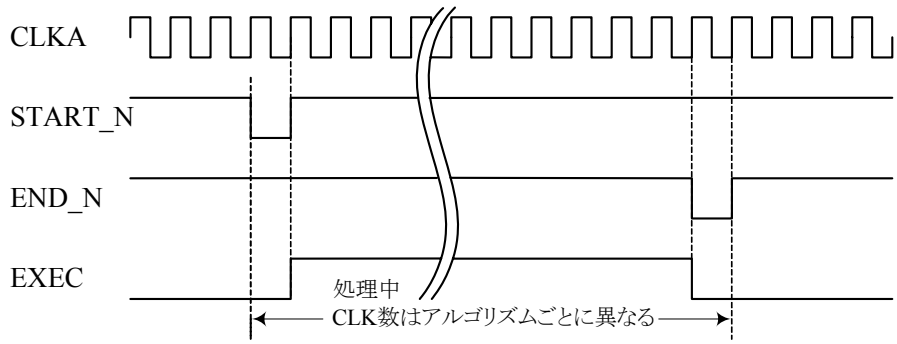


図 4　暗号処理のタイミングチャート

3. 内部詳細仕様

3.1 LSI 内部構成

暗号 LSI の全体ブロック図を図 5 に，また各暗号 IP のソースコードの階層構造を図 6 に示す．暗号 LSI は表 4 の 13 種類の暗号 IP コアとインタフェース回路から構成されている．各暗号 IP の仕様は，下記の東北大学大学院情報科学研究科青木研究室の Web サイトを参照のこと．

http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html

表 4 暗号 IP コア

IP	IP コア名	内容
0	AES_Comp	合成体による S-box を用いた AES 実装．128 ビット鍵による暗号化と復号をサポート．
1	AES_Comp_ENC_top	AES_Comp の暗号化部のみの実装．
2	AES_TBL	S-box を case 文で記述したもの AES 実装．128 ビット鍵による暗号化のみサポート．
3	AES_PPRM1	Positive Prime Reed-Muler 論理による 1 段の AND-XOR ロジックで S-box を記述した AES 実装．128 ビット鍵による暗号化のみサポート．
4	AES_PPRM3	Positive Prime Reed-Muler 論理による 3 段の AND-XOR ロジックで S-box を記述した AES 実装．128 ビット鍵による暗号化のみサポート．
5	DES	56 ビット鍵による 64 ビットブロック暗号の Single DES．
6	MISTY1	128 ビット鍵による 64 ビットブロック暗号．S-box S7 と S9 は case 文で記述．
7	Camellia	128 ビットブロック暗号 Camellia．S-box は case 文で記述．
8	SEED	128 ビット鍵による 64 ビットブロック暗号 SEED．
9	CAST128	128 ビット鍵による 64 ビットブロック暗号 CAST128．
10	RSA	32 ビット乗算器による Montgomery 乗算を用いた RSA 暗号．
11	AES_SSS1	AES_Comp_Enc_top と同等の回路に，標準ライブラリで RSL(Random Switching Logic)を模擬した擬似 RSL による DPA 対策を施したもの．
12	AES_S	AES_Comp と同じ RTL ソースを用い，FPGA(Xilinx Virtex2)と同等のノードを持つネットリストとなるように制約を与えて論理合成したもの．

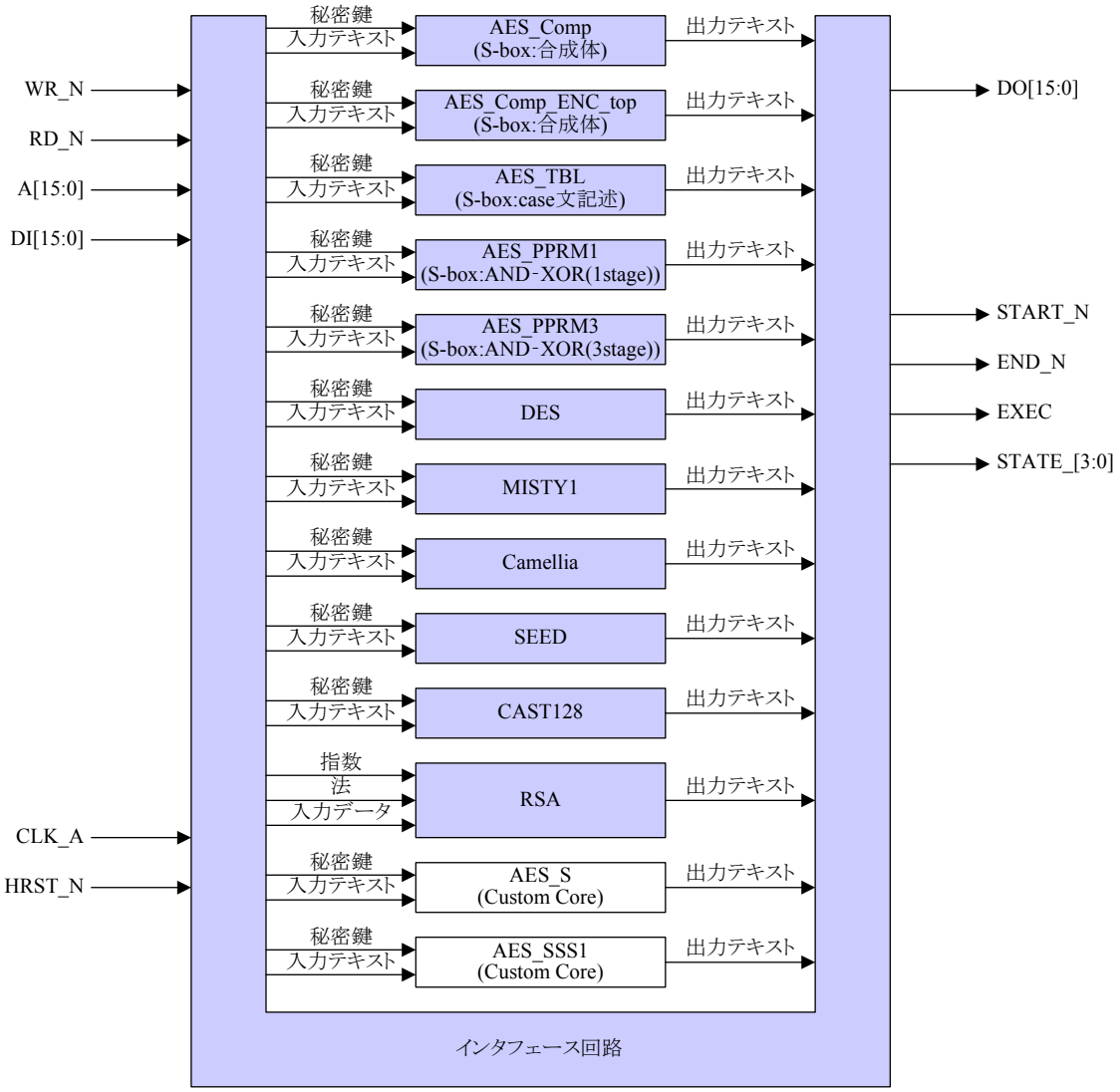

WR_N
RD_N
A[15:0]
DI[15:0]
CLK_A
HRST_N
秘密鍵
入力テキスト
AES_Comp
(S-box:合成体)
AES_Comp_ENC_top
(S-box:合成体)
AES_TBL
(S-box:case文記述)
AES_PPRM1
(S-box:AND-XOR(1stage))
AES_PPRM3
(S-box:AND-XOR(3stage))
DES
MISTY1
Camellia
SEED
CAST128
指数
法
入力データ
RSA
AES_S
(Custom Core)
AES_SSS1
(Custom Core)
出力テキスト
インタフェース回路
DO[15:0]
START_N
END_N
EXEC
STATE_[3:0]

図 5 全体ブロック図

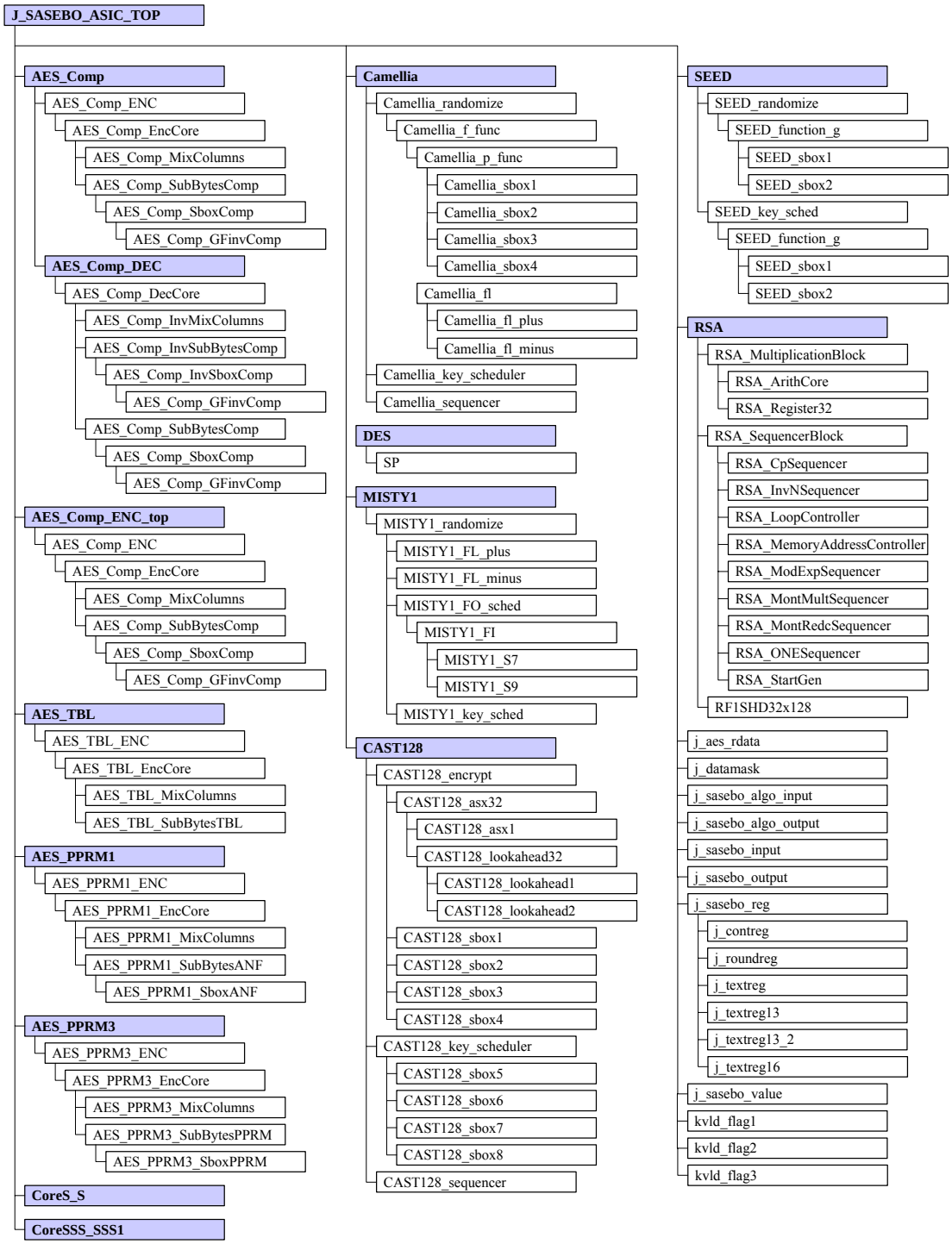

J_SASEBO_ASIC_TOP
AES_Comp
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColumns
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
AES_Comp_DEC
AES_Comp_DecCore
AES_Comp_InvMixColumns
AES_Comp_InvSubBytesComp
AES_Comp_InvSboxComp
AES_Comp_GFinvComp
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
AES_Comp_ENC_top
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColumns
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
AES_TBL
AES_TBL_ENC
AES_TBL_EncCore
AES_TBL_MixColumns
AES_TBL_SubBytesTBL
AES_PPRM1
AES_PPRM1_ENC
AES_PPRM1_EncCore
AES_PPRM1_MixColumns
AES_PPRM1_SubBytesANF
AES_PPRM1_SboxANF
AES_PPRM3
AES_PPRM3_ENC
AES_PPRM3_EncCore
AES_PPRM3_MixColumns
AES_PPRM3_SubBytesPPRM
AES_PPRM3_SboxPPRM
CoreS_S
CoreSSS_SSS1
Camellia
Camellia_randomize
Camellia_f_func
Camellia_p_func
Camellia_sbox1
Camellia_sbox2
Camellia_sbox3
Camellia_sbox4
Camellia_fl
Camellia_fl_plus
Camellia_fl_minus
Camellia_key_scheduler
Camellia_sequencer
DES
SP
MISTY1
MISTY1_randomize
MISTY1_FL_plus
MISTY1_FL_minus
MISTY1_FO_sched
MISTY1_FI
MISTY1_S7
MISTY1_S9
MISTY1_key_sched
CAST128
CAST128_encrypt
CAST128_asx32
CAST128_asx1
CAST128_lookahead32
CAST128_lookahead1
CAST128_lookahead2
CAST128_sbox1
CAST128_sbox2
CAST128_sbox3
CAST128_sbox4
CAST128_key_scheduler
CAST128_sbox5
CAST128_sbox6
CAST128_sbox7
CAST128_sbox8
CAST128_sequencer
SEED
SEED_randomize
SEED_function_g
SEED_sbox1
SEED_sbox2
SEED_key_sched
SEED_function_g
SEED_sbox1
SEED_sbox2
RSA
RSA_MultiplicationBlock
RSA_ArithCore
RSA_Register32
RSA_SequencerBlock
RSA_CpSequencer
RSA_InvNSequencer
RSA_LoopController
RSA_MemoryAddressController
RSA_ModExpSequencer
RSA_MontMultSequencer
RSA_MontRedcSequencer
RSA_ONESequencer
RSA_StartGen
RF1SHD32x128
j_aes_rdata
j_datamask
j_sasebo_algo_input
j_sasebo_algo_output
j_sasebo_input
j_sasebo_output
j_sasebo_reg
j_contreg
j_roundreg
j_textreg
j_textreg13
j_textreg13_2
j_textreg16
j_sasebo_value
kvld_flag1
kvld_flag2
kvld_flag3

図 6 階層構造

3.2 外部インタフェース

図 7 および図 8 に共通鍵暗号, 図 9 および図 10 に RSA 暗号の外部インタフェース回路を示す.

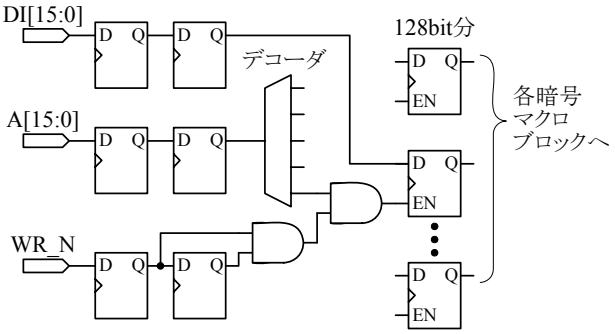


図 7 共通鍵暗号アルゴリズムのライト側インタフェース回路

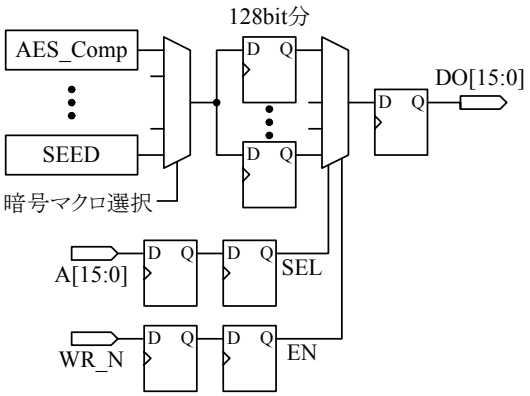


図 8 共通鍵暗号アルゴリズムのリード側インタフェース回路

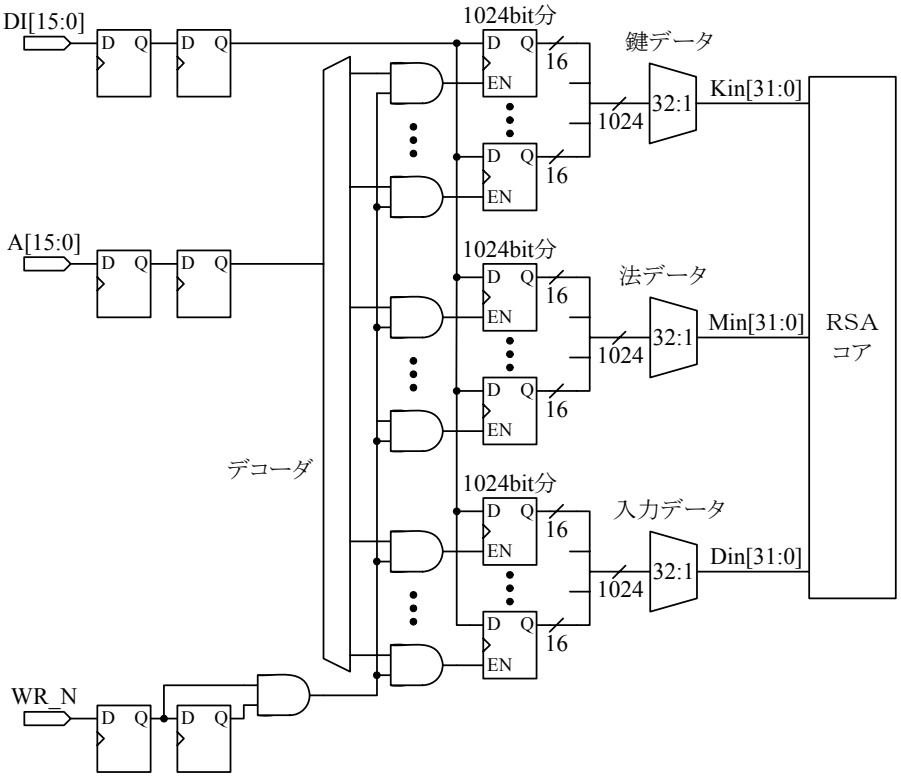


図 9　RSA 暗号のライト側インタフェース回路

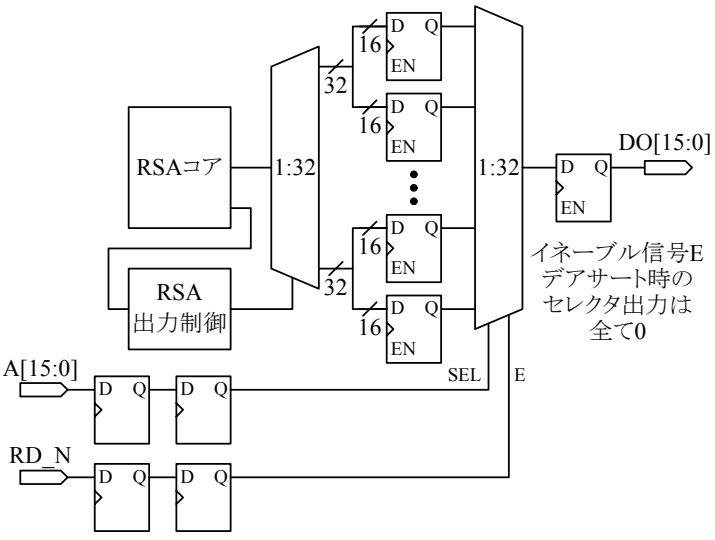


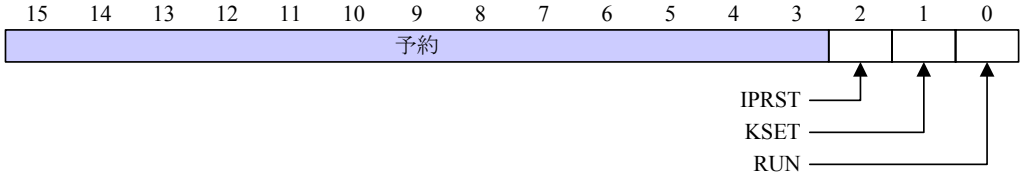
図 10　RSA 暗号のリード側インタフェース回路

3.3 インタフェースレジスタ

本節では各インタフェースレジスタの詳細について説明する.

- **コントロールレジスタ:CONT**

本レジスタは暗号処理の開始と終了に関連する.



Bit 0:RUN

1 を書き込むことで, IP 選択レジスタ(IPSEL)で指定した暗号 IP が 16 クロック後に動作を開始する. 出力選択レジスタ(OUTSEL)で指定した暗号 IP による処理が終了し, 出力テキスト/データレジスタ(OTEXT/ODATA)の読み出しが可能になると, 本ビットは自動的に 0 クリアされる. 本ビットが 1 の期間中は, 全てのレジスタへの書き込みは原則禁止とし, 出力テキスト/データレジスタから読み出される値は無効である.

Bit 1:KSET

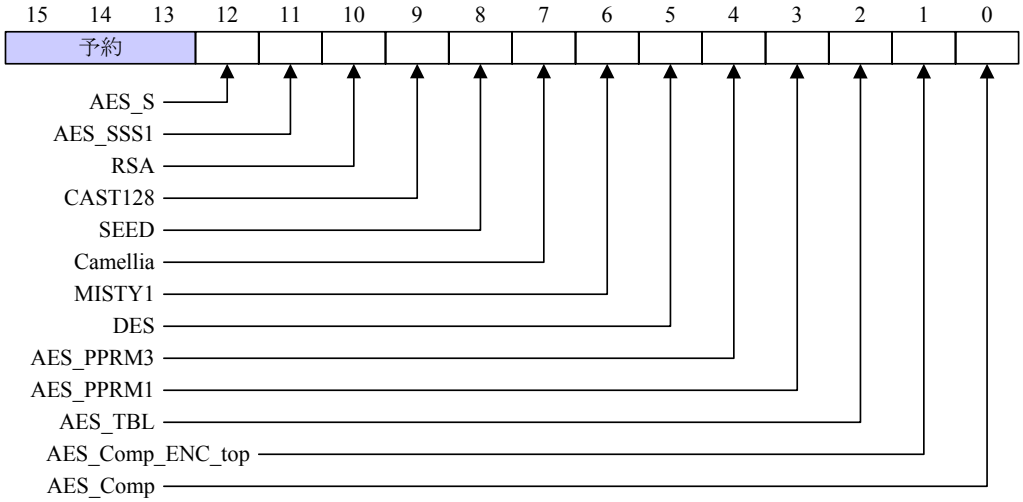
1 を書き込むことで, IP 選択レジスタ(IPSEL)で指定した暗号 IP に, モードレジスタ MODE に応じた鍵生成(鍵設定)が行われる. 出力選択レジスタ(OUTSEL)で指定した暗号 IP の鍵生成(鍵設定)が終了し, 設定された鍵を用いた暗号処理が可能になると, 本ビットは自動的に 0 クリアされる. 本ビットが 1 の期間中は, 全てのレジスタへの書き込みは原則禁止とする. 特に, 本ビットが 1 の期間中に RUN ビットをセットした場合の動作は保証されない.

Bit 2:IPRST

1 を書き込むことで, IP 選択レジスタ(IPSEL)で指定した暗号 IP をリセットする. 0 を書き込むことで, 同上の暗号 IP のリセットを解除する. 本ビットの初期値は 1 である.

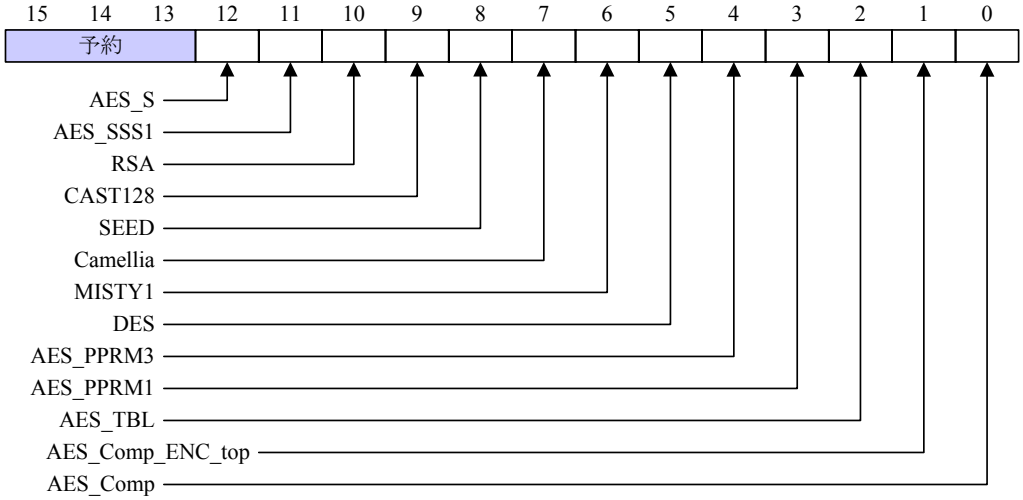
- **IP 選択レジスタ:IPSEL**

13 個の暗号 IP のうち, IP 選択レジスタの対応するビットに 1 がセットされたもののみが active 状態となり, 選択 IP 以外にはクロックは供給されない.



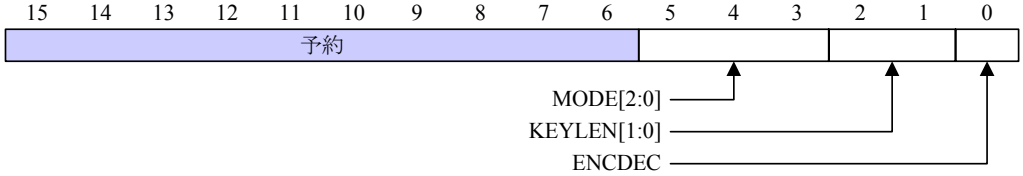
- **出力選択レジスタ:OUTSEL**

IP 選択レジスタ(IPSEL)の対応するビットに 1 をセットすることで, active 状態となった暗号 IP のうち演算結果を出力する暗号 IP を指定する. 出力選択レジスタの対応するビットに 1 がセットされた暗号 IP の演算結果が, 出力テキスト/データレジスタ(OTEXT/ODATA)に格納される. 出力選択レジスタの複数のビットに 1 をセットした場合の出力値は保証されない.



- **モードレジスタ:MODE**

動作モード, 鍵長, 暗号化/復号を指定する.



Bit 5-3:MODE[2:0]

値は 000 に固定されており, ECB(Electoric Code Book)モードのみサポートしている.

Bit 2-1:KEYLEN[1:0]

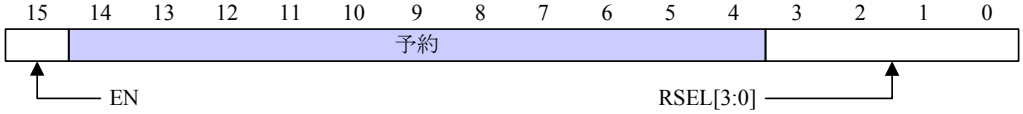
値は 00 に固定されており, IP 毎に決まっている鍵長が用いられる.

Bit 0:ENCDEC

0 で暗号化, 1 で復号を行う. 暗号化のみの IP(IP1~4, IP11, IP12)が選択された場合, このビットは意味を持たない. また DES だけは, 1 が暗号化, 0 が復号となっている.

- **ラウンド選択レジスタ:RSEL**

中間値レジスタ(RDATA0-RDATA7)に値を取り込むラウンド数を指定する. RSEL, RDATA0~RDATA7 は, active な暗号 IP として AES_Comp が選択されているときだけ意味を持つ.



Bit 15:EN

0: 中間値を取り込むための回路の動作を抑制する(クロックを供給しない).

1: 中間値を取り込むための回路を活性化する(クロックを供給する).

Bit 3-0:RSEL[3:0]

中間値レジスタ(RDATA0~RDATA7)に中間データを格納すべきラウンド数.

- **テストレジスタ 1:TEST1**

テストレジスタ 1 は AES_SSS1 コア，および AES_S コアのモード制御を行うデバッグ用レジスタである．仕様は非公開とする．

- **テストレジスタ 2:TEST2**

テストレジスタ 2 は AES_SSS1 コアの制御を行うデバッグ用レジスタである．仕様は非公開とする．

- **共通鍵暗号用鍵レジスタ:KEY0~7**

鍵レジスタは，選択されている IP が使用する入力鍵データを設定する．KEY0 に最上位 16 ビット分の鍵を，以下 KEY1，KEY2，・・・と入力していく．鍵長は DES の 56 ビットを除き，全ての共通鍵暗号の IP は 128 ビットである．選択暗号 IP が DES の場合は図 11 のように，KEY4~7 に 56 ビット鍵データを下詰めで設定し，KEY0~3 および KEY4 の上位 8 ビットは全て 0 を設定する．

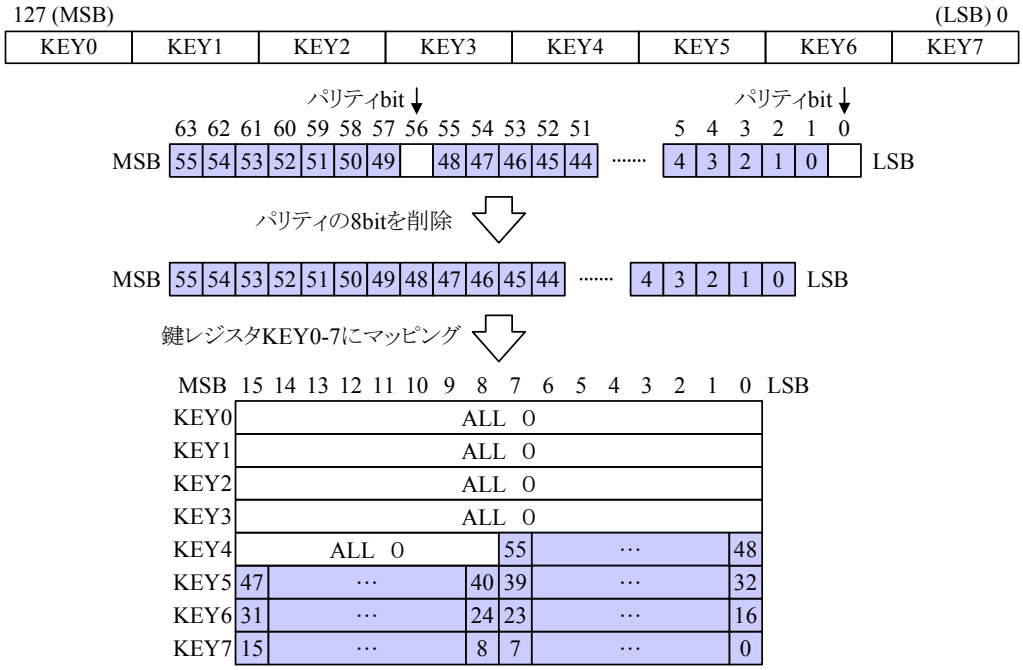
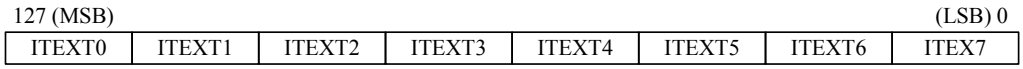


図 11　DES コア鍵データビットアサイン

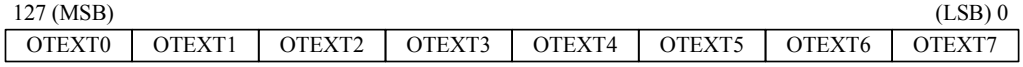
- **共通鍵暗号用入力テキストレジスタ:ITEXT0~7**

入力テキストデータを 16 ビットずつ上位から ITEXT0，ITEXT1，ITEXT2，・・・の順番に書き込む．64 ビットブロック暗号は ITEXT0~4 を使用する．



- **共通鍵暗号用出力テキストレジスタ:OTEXT0~7**

出力テキストデータを 16 ビットずつ上位から OTEXT0，OTEXT1，OTEXT2，・・・の順番に読み出す．64 ビットブロック暗号は OTEXT0~4 を使用する．



- **共通鍵暗号用中間値レジスタ:RDATA0~7**

入力テキストデータの書き込み, 出力テキストデータと中間値データの読み出しのためのレジスタ群である. ITEXT0/OTEXT0/RDATA0 に最上位 16 ビット分のデータが保持され, 以下 ITEXT1/OTEXT1/RDATA1, ITEXT2/OTEXT2/RDATA2, …と続く. IP 毎に必要な鍵のビット分のみを使用する. なお, 中間値レジスタは, active な暗号 IP として AES0 が選択されているときだけ意味を持つ.

127 (MSB) (LSB) 0

RDATA0	RDATA1	RDATA2	RDATA3	RDATA4	RDATA5	RDATA6	RDATA7

- **公開鍵暗号用指数レジスタ:EXP00-3F**
- **公開鍵暗号用法レジスタ:MOD00-3F**
- **公開鍵暗号用入力データレジスタ:IDATA00-3F**
- **公開鍵暗号用出力データレジスタ:ODATA00-3F**

公開鍵暗号用の指数と法の設定, 入力データの書き込み, 及び出力データの読み出しのためのレジスタ群である. 酢数データは 16 ビットずつ上位から, EXP00, EXP01, EXP02, ・・・の順に入力し, 他のデータも同様に上位から 00, 01, 02, ・・・と設定または読み出しを行う.

- **バージョンレジスタ:VER**

暗号 LSI のバージョンを表す読み出し専用レジスタ. 国内向 LSI は固定値 0x0F5A, 輸出用 LSI は固定値 0xC381 が読み出される.

3.4 クロックツリー

暗号 LSI では，IP 選択レジスタ IPSEL を設定することで，測定対象とするコアにだけ動作クロックを供給することができる．図 12 のようにクロック回路はゲーティッドクロック構成とし，LSI の配置配線時に遅延制御を行って，複数のクロックを同一位相のクロックとして取り扱えるようにしている．

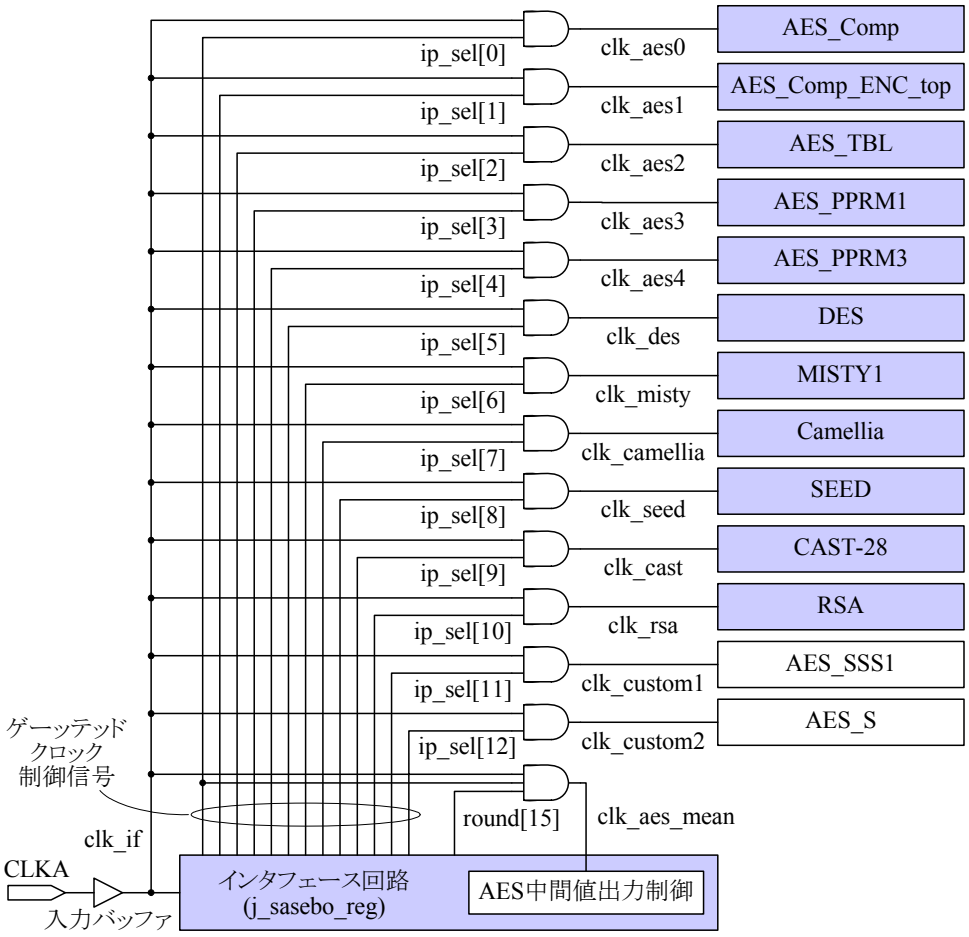


図 12 クロック系統図

3.5 リセット

図 13 は評価用 LSI のリセット系統であり，リセットシーケンスは以下の通りである．なお，IP 選択レジスタで選択されていない IP にはクロックが供給されず，リセット信号がアサートされたままであることに注意が必要である．

① HRST_N アサート/デアサート

HRST_N 信号をアサートすることにより，インタフェース回路がリセットされる．このときインタフェース回路のコントロールレジスタ CONT 内 IPRST ビットは 1 にセットされ，各 IP のリセット信号がすべてアサートされる．その後，HRST_N 信号をデアサートする．この状態が暗号 LSI の初期状態である．

② CLK_A 入力

インタフェース回路が動作可能な状態となる．この時点で，各 IP にクロックは供給されておらず，リセット信号もアサートされたままである．

③ IP コア選択

インタフェース回路の IP 選択レジスタ IPSEL 中の該当ビットをセットし，動作させる IP を選択する．IPSEL で選択されたコアに対してクロックが供給される．この時点では，選択されたコアを含め各コアへのリセット信号はアサートされたままである．

④ 選択したコアのリセット解除

インタフェース回路のコントロールレジスタ CONT 中の IPRST ビットに 0 を書き込むことで，③で選択したコアのリセット信号がデアサートされ，リセットが解除される．なおリセットシーケンスではないが，この後に出力選択レジスタ OUTSEL も設定しておく必要がある．

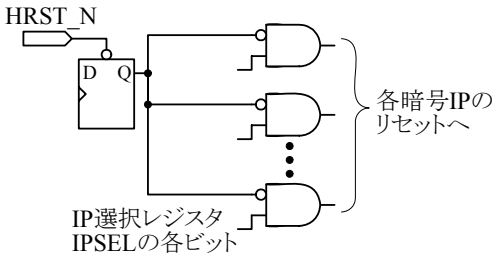


図 13 リセット系統

3.6 付帯機能

- **鍵長制限**

暗号 LSI は表 5 に示したように，国内用と海外用として，サポートしている鍵長が異なる 2 種類の設計・製造を行った．共通鍵ブロック暗号は DES を除き 128 ビットの鍵であるが，海外用は図 14 のように上位 72 ビットを“0x00010203040506070 8”に固定しており，ユーザは下位 56 ビットだけを設定することが可能で，上位 72 ビットはデータを書き込んでも無視される．なお，AES_SSS1 と AES_S は国内用/海外用に関わらず鍵長が 56 ビットに制限されている．

また，RSA の鍵長である指数は国内用が 1,024 ビット，海外用が 512 ビットである．海外用は指数以外にも法と入力データも 512 ビットに制限されており，これらのレジスタに 1,024 ビット設定しようとしても上位 512 ビットは無視されて 0 で埋められる．

表 5 国内用と海外用の暗号 LSI がサポートする鍵長

IP	国内用	海外用
DES	アルゴリズム鍵 56bit 中 56bit 設定可．ビットアサインについては図 11 を参照．	同左
AES_Comp/ AES_Comp_ENC_top/ AES_TBL/AES_PPRM1/ AES_PPRM3/MISTY1/ Camellia/SEED/CAST128	アルゴリズム鍵 128bit 中 128bit 設定可．	アルゴリズム鍵 128bit 中 56bit のみ設定可能．固定値の 72bit は図 14 を参照．
AES_SSS1 AES_S	アルゴリズム鍵 128bit 中 56bit のみ設定可能．固定値の 72bit は図 14 を参照．	アルゴリズム鍵 128bit 中 56bit のみ設定可能．固定値の 72bit は図 14 を参照．
RSA	指数，法，入力データ共に 1,024bit 設定可能．	指数，法，入力データ共に 512bit に制限．上位 512bit は 0 に固定．

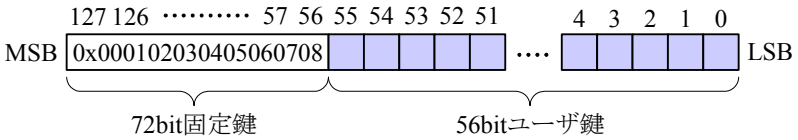


図 14 鍵データビットアサイン

- **遅延実行**

暗号 LSI の暗号処理中の電力波形を精度よく観測できるように，鍵設定やデータ入出力と暗号処理の時間をずらしている．具体的には，コントロールレジスタ CONT の RUN ビットを設定して処理開始を指示してから，16 クロック後に暗号 IP の処理開始信号がアサートされるようになっている．

- **ノイズ発生源**

対象とする暗号 IP 以外の IP をノイズ発生源として利用し，電力解析や電磁波解析に与える影響を評価することが可能である．具体的には，IP 選択レジスタ IPSEL で複数の暗号 IP を選択し，出力選択レジスタ OUTSEL で評価対象の IP だけを選択することで実現される．

4. LSI の物理レイアウト

暗号 LSI の論理合成後のレイアウト情報について説明する. 表 6 は LSI の概要であり, 130nm の CMOS プロセスによる 5×5 mm^2 のダイサイズのうち, 10.54%のゲートを使用している. 図 15 の左に示したようにモジュール内のタイミングを改善するために中央に集中して配置させた結果, SRAM や外部インタフェース部にタイミング違反と容量違反が多数発生した. そこで, 図 15 右のように LSI 全体に分散配置することとした. また, このように分散することによって暗号モジュールのエリアが明確に分割され, クロストークが改善される. 目標の動作周波数は 24MHz であるが, レイアウト時のタイミング修正を容易にするため, 30%のマージンを加え 31MHz で論理合成を行った. また多くの Setup マージンを確保するため, 入出力にも大きな遅延を与えている.

表 6 暗号 LSI の概要

項目	
ウェハプロセス	TSMC CL013G 130nm CMOS, アルミ 6 層配線
コア電源電圧	1.2±0.05V
I/O 電源電圧	3.3±0.16V
動作周波数	24MHz (41ns)
データエリア	5 × 5 mm^2
ゲート使用率	10.54%
PAD 数	160 個
品持セル	SRAM

表 7 使用 EDA Tool

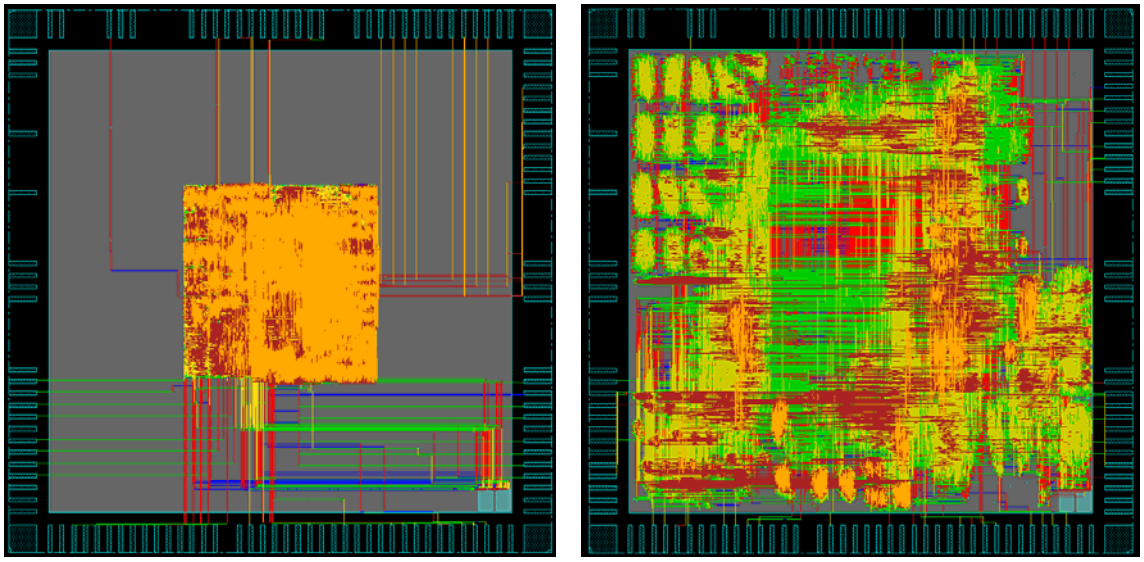
用途	ソフト名	ベンダー	バージョン
論理合成	Design Compiler	Synopsys	Y-2006.06-SP5-1
配置・配線	SOC Encounter	Cadence	SOC62USR1
RC 抽出	Star-RCXT	Synopsys	2006.12-SP1
クロストーク抽出	CeltIC	Cadence	SOC41USR3
STA	PrimeTimeSI	Synopsys	X-2006.12-SP2
レイアウト検証	Calibre	Mentor	v2007.1_24.22
Power 検証	AstroRail	Synopsys	Y-2006.06-SP5
等価検証	Formality	Synopsys	Z-2007.06-SP1

表 8 使用ライブラリ

分類	ライブラリ	バージョン
Standard Cell	SAGE-X Standard Cells (TSMC CL013G) FB	2007q1v2
	SAGE-X Standard Cells (TSMC CL013G) FX – CeltIC	2005q3v1
Digital I/O	ZBond I/O, TPZ013G3, 1.2V/3.3V, 5V (TSMC CL013G) FB	210c
RAM	SP-RF HSD - 1.0V (TSMC CL013G) FB 2007q1v1	2007q1v1
LVS Rule	LVS_RC_Calibre_0.13 μm _LOGIC_1p8m_1.2V+2.5V_V21d	T-013-LO-SP-004-C1

表 9 論理合成条件

条件項目	条件値
動作周波数	31MHz (32ns) 24MHz+30%マージン
入力遅延	20ns
出力遅延	20ns
外部負荷容量	20pf



(a) 集中配置　　(b) 分散配置

図 15　暗号 LSI のフロアプラン

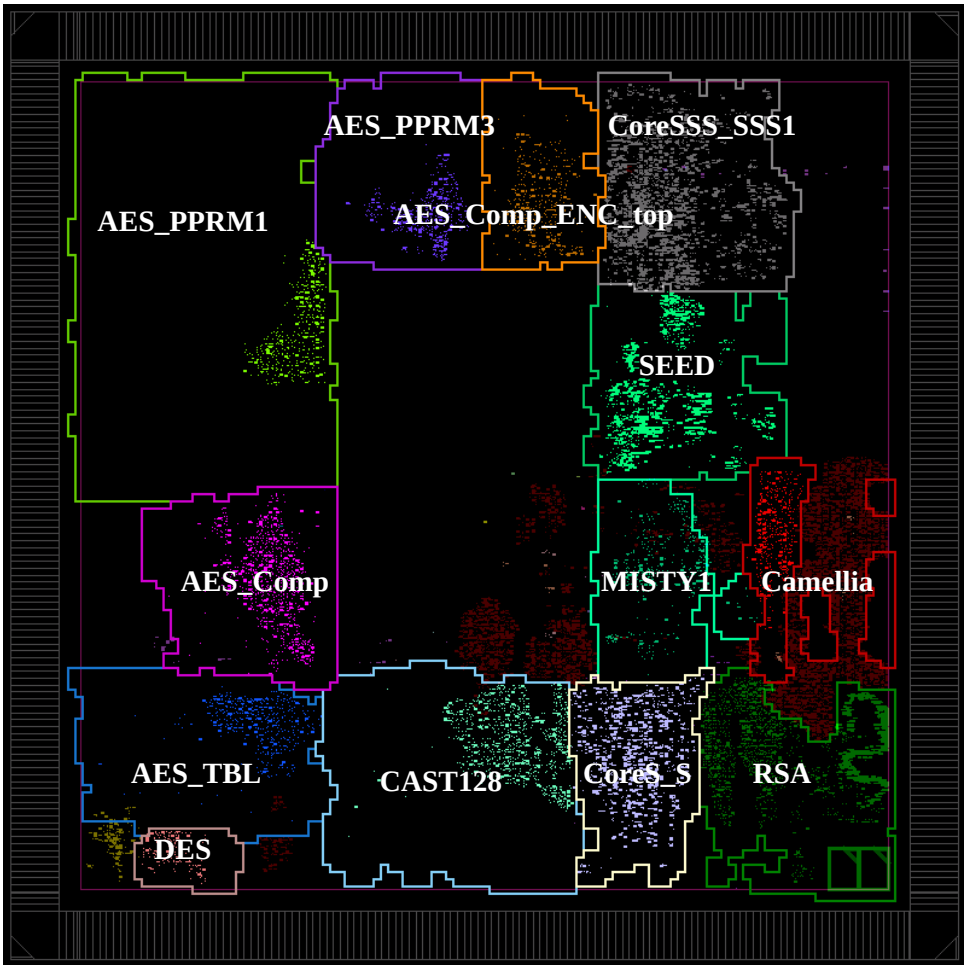


図16　暗号モジュール配置図

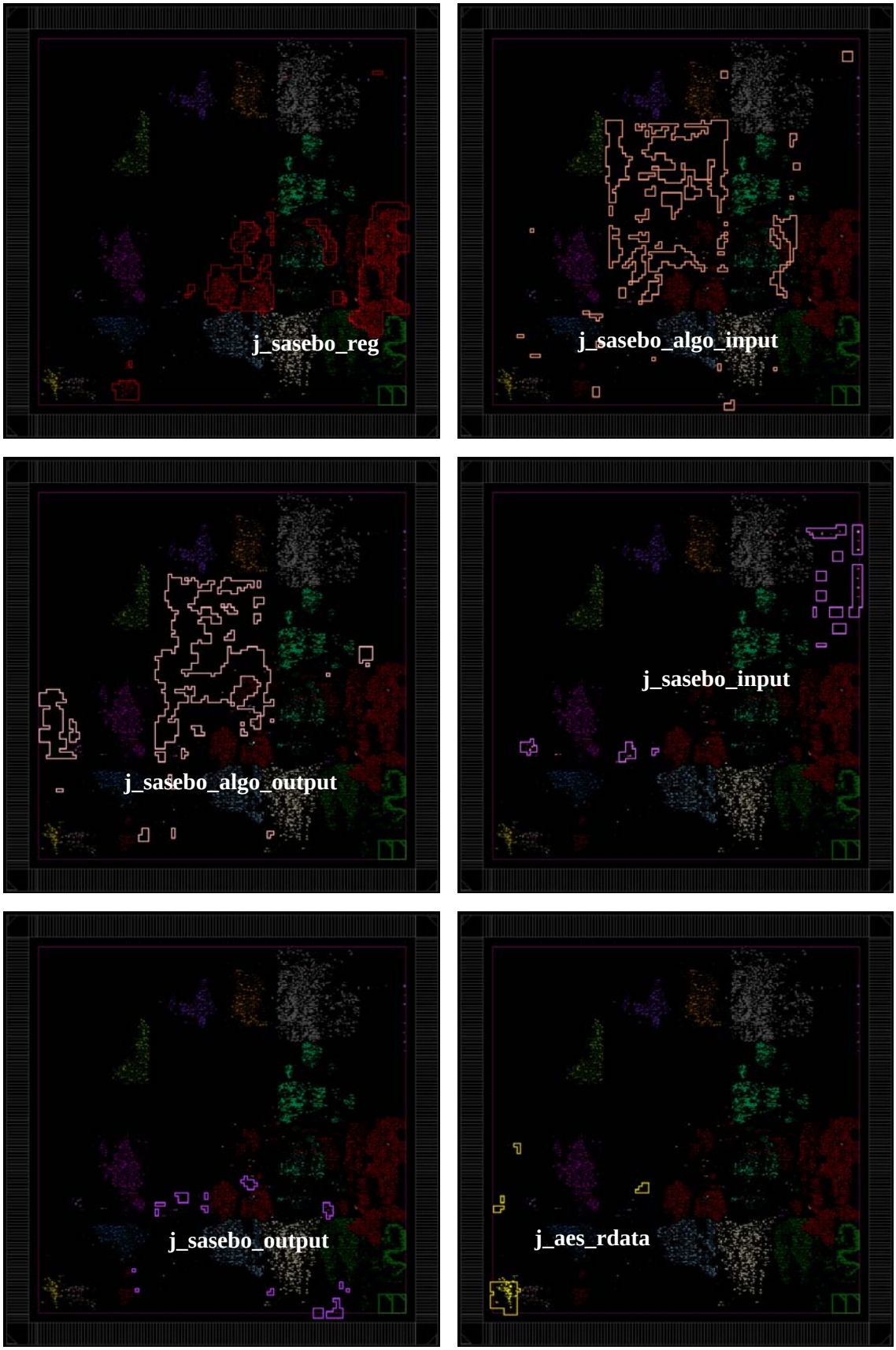


図17　データ入出力モジュール配置図

図 16 は各暗号モジュールの配置を，図 17 はデータ入出力モジュールの配置を示している．また，表 10 はそれらモジュールの回路規模の一覧である．また，表 11 は Worst(125℃ 1.08V), Typical(25℃ 1.20V), Best(-40℃ 1.32V)各条件下において，ターゲットを 41ns cycle (24MHz)とした場合の LSI の速度性能で，表 2.12 は暗号モジュール毎の Slack 値を示したものである．Setup タイミングが最も厳しいのが AES_SSS1 の 6.219ns で，サイクル時間は 34.781ns (=41ns - 6.219ns)で最大動作周波数は 28.75MHz(=1/34.781ns)である．また，最も緩いのが DES の 31.984ns で，サイクル時間 9.016ns (=41ns - 31.98ns)で最大動作周波数は 110.9MHz (=1/9.016)であった．

表 10 モジュール面積一覧

ブロック名	面積 (μm^2)	面積 (%)	ゲート数
AES_Comp	125,240.96	7.09	24,595
AES_Comp_ENC_top	58,964.28	3.34	11,579
AES_PPRM1	284,243.20	16.08	55,819
AES_PPRM3	74,522.65	4.22	14,635
AES_TBL	101,210.87	5.73	19,876
CAST128	151,330.00	8.56	29,718
SEED	133,020.15	7.53	26,122
DES	16,067.59	0.91	3,155
RSA	102,663.84	5.81	20,161
Camellia	71,394.34	4.04	14,020
MISTY1	86,854.26	4.91	17,056
CoreS_S	76,669.86	4.34	15,056
CoreSSS_SSS1	158,370.81	8.96	31,101
J_sasebo_reg	206,758.59	11.70	40,603
J_sasebo_algo_input	54,754.73	3.10	10,753
J_sasebo_algo_output	24,561.38	1.39	4,823
J_sasebo_input	2,671.71	0.15	525
J_sasebo_output	12,121.13	0.69	2,380
J_aes_rdata	6,816.76	0.39	1,339
J_sasebo_value	880.95	0.05	173
J_SASEBO_ASIC_TOP	18,062.03	1.02	3,547
Total cell area	1767,180.09	100.00	34,7037

1 ゲート = 2 入力 NAND(NAND2X1: 3.69μm × 1.38μm)

表 11 Static Timing Analysis による LSI の動作速度 (Target 41ns cycle)

動作条件	Worst (125℃ 1.08V)	Typical (25℃ 1.20V)	Best (-40℃ 1.32V)
最大動作周波数	27.63MHz (36.19ns)	32.38MHz (30.88ns)	35.88MHz (28.87ns)
Setup (slack)	4.81ns	10.12ns	13.13ns
Hold (slack)	0.20ns	0.10ns	0.02ns

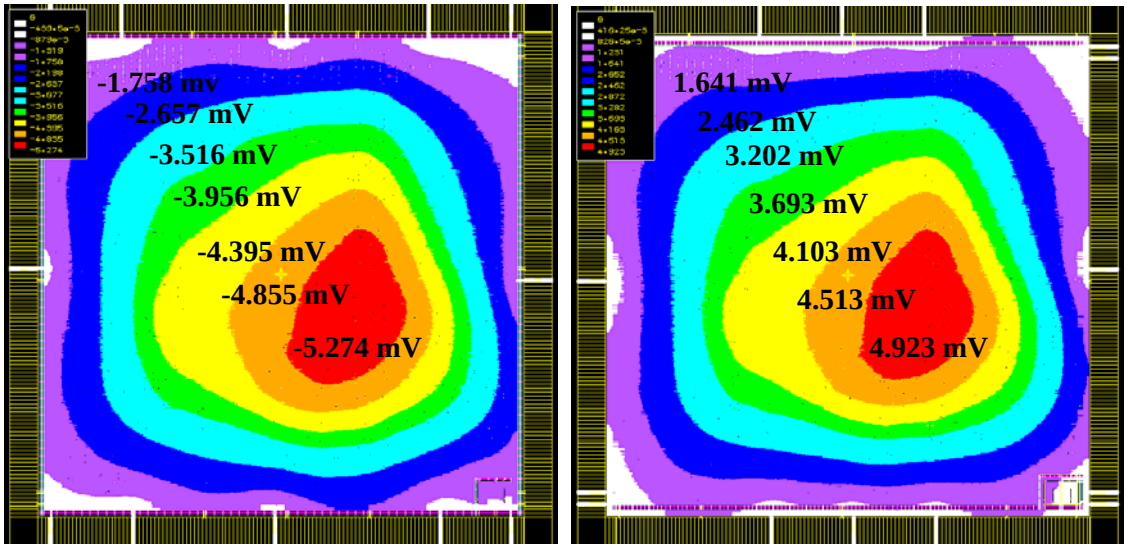
表 12 Static Timing Analysis による各暗号モジュールの Slack 値 (Target 41ns cycle)

ブロック名	Worst		Typical		Best	
	Hold (ns)	Setup (ns)	Hold (ns)	Setup (ns)	Hold (ns)	Setup (ns)
AES_Comp	0.399	21.265	0.227	27.212	0.110	31.512
AES_Comp_ENC_top	0.432	25.988	0.264	30.433	0.136	33.743
AES_PPRM1	0.310	18.980	0.188	25.593	0.093	30.493
AES_PPRM3	0.415	27.741	0.236	31.593	0.115	34.500
AES_TBL	0.393	30.708	0.228	33.591	0.116	35.721
CAST128	0.456	11.957	0.273	20.737	0.132	27.145
SEED	0.317	7.675	0.173	17.902	0.075	25.444
DES	0.441	31.984	0.266	34.501	0.140	36.357
RSA	0.401	11.952	0.251	21.250	0.117	27.849
Camellia	0.446	24.189	0.278	28.954	0.147	32.614
MISTY1	0.450	7.144	0.275	17.380	0.144	25.017
AES_S	0.495	25.803	0.267	30.388	0.134	33.631
AES_SSS1	0.343	6.219	0.202	10.116	0.088	13.126

表 13 は全セルのうち 30%が活性化したと仮定した場合の消費電力と電力降下で，図 18 は VDD 側と VSS 側のコア電源プレーンの電圧降下のイメージである．電圧降下は 0.44%と極めて小さい上，実際には 13 個のマクロのうち一度に 1 つしか動作しないので，まったく問題ない値である．

表 13　VDD/VSS 電圧降下

	VDD	VSS
動作周波数	24 MHz	
遷移確率	30 %	
消費電力	51.21 mW	
Worst drop 値	5.273 mV	4.923 mV
Drop 率	0.439 %	0.410 %



(a) IR-DROP(VDD)　　(b) IR-DROP(VSS)

図 18　VDD/VSS の電圧降下

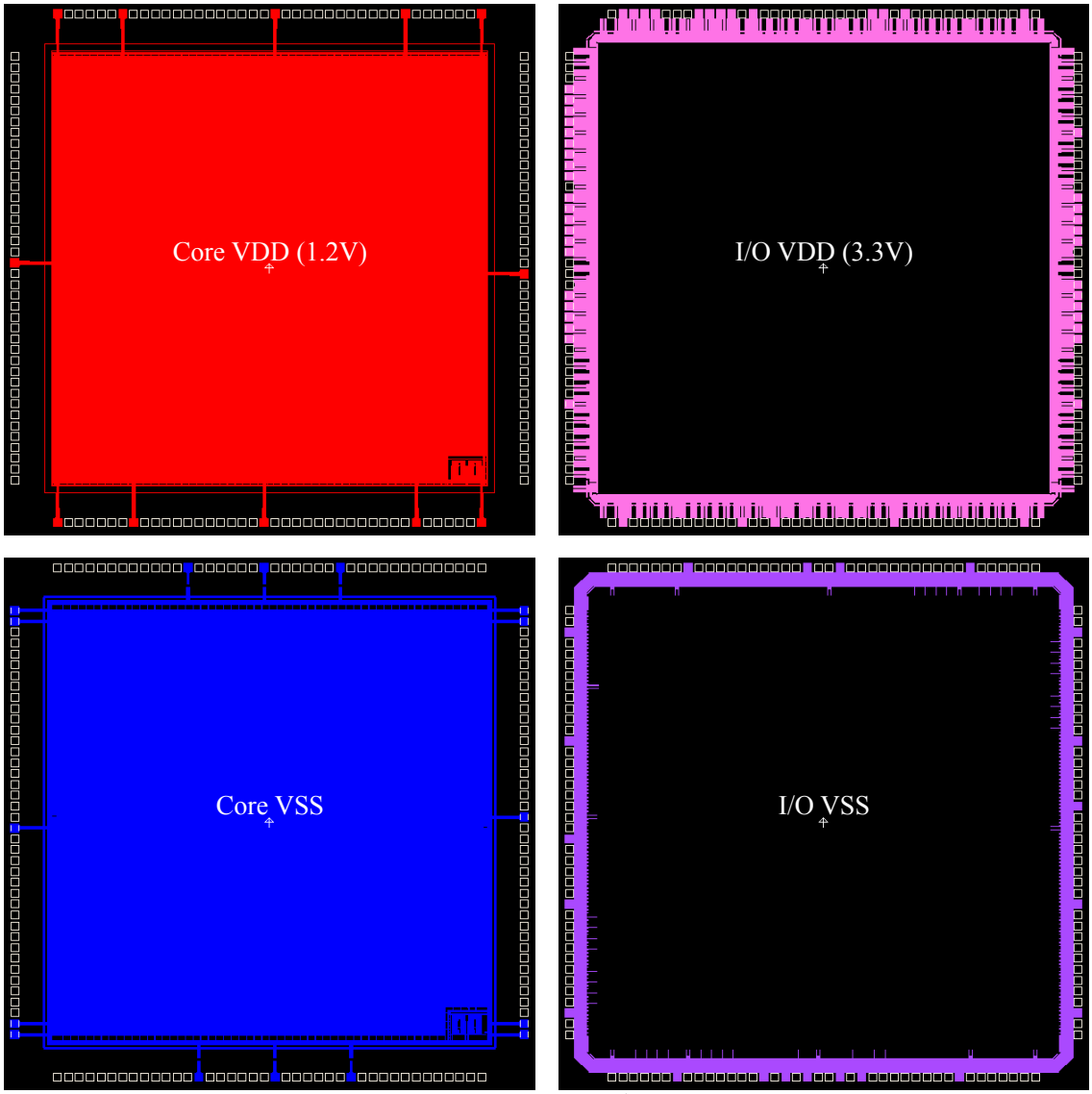


図19　電源ラインの配線パターン

※1　本ボードの著作権は(独)産業技術総合研究所に，本仕様書の著作権は経済産業省に帰属します．

※2　本ボードおよび本仕様書の全部または一部を，著作権者に無断で複写，複製することはできません．

※3　ボードおよび本仕様書は，個人として利用するほかは，著作権者に無断で使用することはできません．

※4　本ボードの仕様は，将来予告なく変更することがあります．

FPGA はザイリンクス社の登録商標です．

その他，記載されている社名・製品名は各社の商標および登録商標です．

【問合せ先】

(独) 産業技術総合研究所　情報セキュリティ研究センター

〒101-002
東京都千代田区外神田 1-18-13 秋葉原ダイビル 11 階 1102 号室
TEL：03-5298-4722
FAX：03-5298-4522