標準暗号 LSI 仕様書
~サイドチャネル攻撃対策版~

Standard Cryptographic LSI Specification
~ with Side Channel Attack Counter Measures ~

[第 1.0 版]

2009 年 8 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

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, 楕円曲線暗号(ECC), 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 130nm および 90nm の CMOS プロセスを用いて製造され, 160 ピン QFP セラミックパッケージで封止されている.

実装したアルゴリズムは下記の 9 種で, AES については異なる 14 種類の実装を行っているため, 計 22 種類の暗号コアの搭載となった. なお, AES の実装⑧~⑬は論理合成をカスタムで行っている. 国内だけでなく海外でも評価実験に使用するため, 輸出規制を受けないよう鍵長に制限を与えている. DES 以外のブロック暗号の秘密鍵 128bit の上位 72bit 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. AES0～AES7/Camellia /CAST/DES/SEED/MISTY1/RSA/T-DES は東北大学大学院情報科学科青木研究室と産業技術総合研究所情報セキュリティ研究センターが, AES8~AES11 は横浜国立大学大学院 環境情報研究院松本研究室が, AES12~AES13 は三菱電機株式会社情報技術総合研究所が, ECC は電気通信大学情報通信工学科太田・崎山研究室がそれぞれ独自に開発したものである. 本事業において学術的研究を促進する目的で無償にて提供を受けているが, これらの暗号回路マクロの著作権は各機関に帰属する. 5 章ではこれら暗号マクロ個々の仕様について解説を行うが, そこに敬意際した仕様書は, 各機関が作成したものに各機関の許可を得て和訳, 加筆・修正を行っている. したがって, それら仕様書の著作権も暗号マクロ毎に, それを作成した研究機関に所属する. なお, 東北大学提供の暗号回路のソースコードおよび英文仕様書は, “Cryptographic Hardware Project” (http://www.aoki.ecei.tohoku.ac.jp/crypto/)からダウンロードすることができる. また 5 章において, サイドチャネル対策を施した AES8~13 の解説は, その対策アルゴリズムの概要を述べるにとどめ, マクロの詳細なデータパスアーキテクチャについては非公開とする.

- AES(鍵長:128bit)
  - ⓪S-Box 実装→合成体, 暗号化/復号サポート
  - ①S-Box 実装→case 文記述, 暗号化のみサポート
  - ②S-Box 実装→AND-XOR 実装(1-Stage), 暗号化のみサポート
  - ③S-Box 実装→AND-XOR 実装(3-Stage), 暗号化のみサポート
  - ④S-Box 実装→合成体, 暗号化のみサポート
  - ⑤CTR モードサポートパイプライン実装
  - ⑥故障攻撃耐性評価用実装
  - ⑦ラウンド鍵を事前計算する実装
  - ⑧DPA 対策評価用実装(Masked AND Operation)
  - ⑨DPA 対策評価用実装(MDPL)
  - ⑩DPA 対策評価用実装(Threshold Implementation)
  - ⑪DPA 対策評価用実装(WDDL)
  - ⑫DPA 対策評価用実装(擬似 RSL)
  - ⑬DPA 対策評価用実装(擬似 RSL の効果評価用)
- Camellia(鍵長:128) 暗号化/復号サポート
- SEED:暗号化/復号サポート
- MISTY1:暗号化/復号サポート
- Triple-DES:3Key, 暗号化/復号サポート
- DES:暗号化/復号サポート
- CAST128:暗号化/復号サポート

- ECC：鍵長は 64bit．標数 2 の体における点のスカラー倍算
- RSA：512bit のべき乗剰余演算

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
- 平成 19 年度に開発された暗号 LSI 専用のサイドチャネル攻撃用標準評価ボード SASEBO-R (Side-channel Attack Standard Evaluation Board)上に実装し，ボード上の FPGA Virtex-II PRO xc2vp30 とインタフェースする機能
- 電力情報等サンプリング用のトリガ信号出力機能．(トリガ信号出力の抑止も可能)
- 故障攻撃時の評価を目的として，事前に設定したアルゴリズム処理の中間値、中間鍵の出力機能(上記⑥の AES コアのみサポート)
- 故障攻撃時の評価を目的として，故障発生時の中間値と中間鍵の出力機能(上記⑥の AES コアのみサポート)
- 0.3 秒毎に自動的に暗号処理を継続する自走モードのサポート(上記⓪の AES コアのみサポート)

2. 外部仕様

2.1 入出力信号

表 2.1 に暗号 LSI の入出力信号の概要を，表 2.2 および図 2.1 に 130nm 版の 160 ピンのアサインを，表 2.3 および図 2.2 に 90nm 版のピンアサインを示す．130nm 版と 90nm 版では，コア電源が異なる以外(1.2V±0.12 および 1.0V±0.1V)は，パッケージ寸法，ピン配置，および論理的インタフェースは同一である．表 2.2 の「Signal Name」中の()は将来の拡張用であることを意味し，暗号 LSI では未使用であり．また，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 2.1 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 の LSI 内部回路用クロック入力．CLKB と全く同一，もしくはより周波数の高いクロックを入力のこと
	CLKB	1	--	IN	LSI インタフェース回路用クロック
	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		77			

表 2.2 130nm 版 LSI 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 2.2 130nm 版 LSI 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	I	3.3V		PDISDGZ	クロック.シュミット
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 2.2 130nm 版 LSI 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 2.2 130nm 版 LSI 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

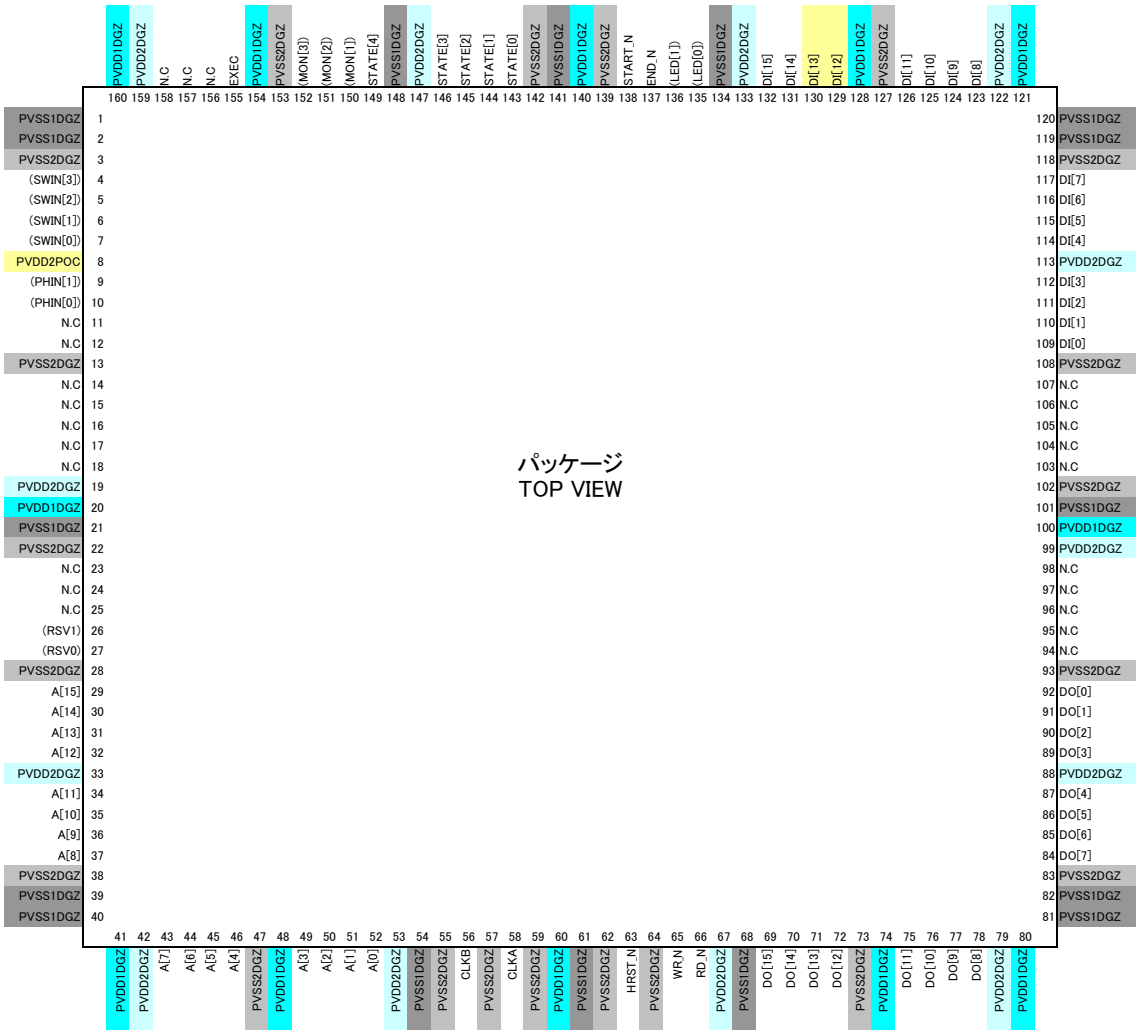


図 2.1　130nm 版暗号 LSI ピンアサインイメージ

表 2.3　90nm 版 LSI ピンアサイン (1/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
1	PVSS1CDG_33					core GND
2	PVSS1CDG_33					core GND
3	PVSS2CDG_33					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_33					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	PVSS2CDG_33					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	PVDD2CDG_33					I/O 3.3V
20	PVDD1CDG_33					core 1.0V
21	PVSS1CDG_33					core GND
22	PVSS2CDG_33					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	PVSS2CDG_33					I/O GND
29	A[15]	I	3.3V		PDC0816CDG_33	アドレスバス
30	A[14]	I	3.3V		PDC0816CDG_33	アドレスバス
31	A[13]	I	3.3V		PDC0816CDG_33	アドレスバス
32	A[12]	I	3.3V		PDC0816CDG_33	アドレスバス
33	PVDD2CDG_33					I/O 3.3V
34	A[11]	I	3.3V		PDC0816CDG_33	アドレスバス
35	A[10]	I	3.3V		PDC0816CDG_33	アドレスバス
36	A[9]	I	3.3V		PDC0816CDG_33	アドレスバス
37	A[8]	I	3.3V		PDC0816CDG_33	アドレスバス
38	PVSS2CDG_33					I/O GND
39	PVSS1CDG_33					core GND
40	PVSS1CDG_33					core GND

表 2.3　90nm 版 LSI ピンアサイン (2/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
41	PVDD1CDG_33					core 1.0V
42	PVDD2CDG_33					I/O 3.3V
43	A[7]	I	3.3V		PDC0816CDG_33	アドレスバス
44	A[6]	I	3.3V		PDC0816CDG_33	アドレスバス
45	A[5]	I	3.3V		PDC0816CDG_33	アドレスバス
46	A[4]	I	3.3V		PDC0816CDG_33	アドレスバス
47	PVSS2CDG_33					I/O GND
48	PVDD1CDG_33					core 1.2V
49	A[3]	I	3.3V		PDC0816CDG_33	アドレスバス
50	A[2]	I	3.3V		PDC0816CDG_33	アドレスバス
51	A[1]	I	3.3V		PDC0816CDG_33	アドレスバス
52	A[0]	I	3.3V		PDC0816CDG_33	アドレスバス
53	PVDD2CDG_33					I/O 3.3V
54	PVSS1CDG_33					core GND
55	PVSS2CDG_33					I/O GND
56	CLKB	I	3.3V		PDS0816CDG_33	クロック.シュミット
57	PVSS2CDG_33					I/O GND
58	CLKA	I	3.3V		PDS0816CDG_33	クロック.シュミット
59	PVSS2CDG_33					I/O GND
60	PVDD1CDG_33					core VDD (1.2V/1.0V)
61	PVSS1CDG_33					core GND
62	PVSS2CDG_33					I/O GND
63	HRST_N	I	3.3V		PDS0816CDG_33	リセット.シュミット
64	PVSS2CDG_33					I/O GND
65	WR_N	I	3.3V		PDC0816CDG_33	書き込み指示
66	RD_N	I	3.3V		PDC0816CDG_33	読み出し指示
67	PVDD2CDG_33					I/O 3.3V
68	PVSS1CDG_33					core GND
69	DO[15]	O	3.3V	8mA	PDC0816CDG_33	出力データ
70	DO[14]	O	3.3V	8mA	PDC0816CDG_33	出力データ
71	DO[13]	O	3.3V	8mA	PDC0816CDG_33	出力データ
72	DO[12]	O	3.3V	8mA	PDC0816CDG_33	出力データ
73	PVSS2CDG_33					I/O GND
74	PVDD1CDG_33					core VDD (1.2V/1.0V)
75	DO[11]	O	3.3V	8mA	PDC0816CDG_33	出力データ
76	DO[10]	O	3.3V	8mA	PDC0816CDG_33	出力データ
77	DO[9]	O	3.3V	8mA	PDC0816CDG_33	出力データ
78	DO[8]	O	3.3V	8mA	PDC0816CDG_33	出力データ
79	PVDD2CDG_33					I/O 3.3V
80	PVDD1CDG_33					core VDD (1.2V/1.0V)

表 2.3　90nm 版 LSI ピンアサイン (3/4)

Pin NO	Signal Name	I/O	I/F Volatage	output	I/O Buffer	Function
81	PVSS1CDG_33					core GND
82	PVSS1CDG_33					core GND
83	PVSS2CDG_33					I/O GND
84	DO[7]	O	3.3V	8mA	PDC0816CDG_33	出力データ
85	DO[6]	O	3.3V	8mA	PDC0816CDG_33	出力データ
86	DO[5]	O	3.3V	8mA	PDC0816CDG_33	出力データ
87	DO[4]	O	3.3V	8mA	PDC0816CDG_33	出力データ
88	PVDD2CDG_33					I/O 3.3V
89	DO[3]	O	3.3V	8mA	PDC0816CDG_33	出力データ
90	DO[2]	O	3.3V	8mA	PDC0816CDG_33	出力データ
91	DO[1]	O	3.3V	8mA	PDC0816CDG_33	出力データ
92	DO[0]	O	3.3V	8mA	PDC0816CDG_33	出力データ
93	PVSS2CDG_33					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	PVDD2CDG_33					I/O 3.3V
100	PVDD1CDG_33					core VDD 1.0V
101	PVSS1CDG_33					core GND
102	PVSS2CDG_33					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	PVSS2CDG_33					I/O GND
109	DI[0]	I	3.3V		PDC0816CDG_33	入力データ
110	DI[1]	I	3.3V		PDC0816CDG_33	入力データ
111	DI[2]	I	3.3V		PDC0816CDG_33	入力データ
112	DI[3]	I	3.3V		PDC0816CDG_33	入力データ
113	PVDD2CDG_33					I/O 3.3V
114	DI[4]	I	3.3V		PDC0816CDG_33	入力データ
115	DI[5]	I	3.3V		PDC0816CDG_33	入力データ
116	DI[6]	I	3.3V		PDC0816CDG_33	入力データ
117	DI[7]	I	3.3V		PDC0816CDG_33	入力データ
118	PVSS2CDG_33					I/O GND
119	PVSS1CDG_33					core GND
120	PVSS1CDG_33					core GND

表 2.3　90nm 版 LSI ピンアサイン (4/4)

Pin NO	Signal Name	I/O	I/F Voltage	output	I/O Buffer	Function
121	PVDD1CDG_33					core 1.0V
122	PVDD2CDG_33					I/O 3.3V
123	DI[8]	I	3.3V		PDC0816CDG_33	入力データ
124	DI[9]	I	3.3V		PDC0816CDG_33	入力データ
125	DI[10]	I	3.3V		PDC0816CDG_33	入力データ
126	DI[11]	I	3.3V		PDC0816CDG_33	入力データ
127	PVSS2CDG_33					I/O GND
128	PVDD1CDG_33					core 1.0V
129	DI[12]	I	3.3V		PDC0816CDG_33	入力データ
130	DI[13]	I	3.3V		PDC0816CDG_33	入力データ
131	DI[14]	I	3.3V		PDC0816CDG_33	入力データ
132	DI[15]	I	3.3V		PDC0816CDG_33	入力データ
133	PVDD2CDG_33					I/O 3.3V
134	PVSS1CDG_33					core GND
135	(LED[0])					N.C
136	(LED[1])					N.C
137	END_N	O	3.3V	8mA	PDC0816CDG_33	暗号処理完了
138	START_N	O	3.3V	8mA	PDC0816CDG_33	暗号処理開始
139	PVSS2CDG_33					I/O GND
140	PVDD1CDG_33					core 1.0V
141	PVSS1CDG_33					core GND
142	PVSS2CDG_33					I/O GND
143	STATE[0]	O	3.3V	8mA	PDC0816CDG_33	選択 IP を示す
144	STATE[1]	O	3.3V	8mA	PDC0816CDG_33	選択 IP を示す
145	STATE[2]	O	3.3V	8mA	PDC0816CDG_33	選択 IP を示す
146	STATE[3]	O	3.3V	8mA	PDC0816CDG_33	選択 IP を示す
147	PVDD2CDG_33					I/O 3.3V
148	PVSS1CDG_33					core GND
149	STATE[4]				PDC0816CDG_33	N.C
150	(MON[1])					N.C
151	(MON[2])					N.C
152	(MON[3])					N.C
153	PVSS2CDG_33					I/O GND
154	PVDD1CDG_33					core 1.0V
155	EXEC	O	3.3V	8mA	PDC0816CDG_33	暗号処理中
156	N.C					N.C
157	N.C					N.C
158	N.C					N.C
159	PVDD2CDG_33					I/O 3.3V
160	PVDD1CDG_33					core 1.0V

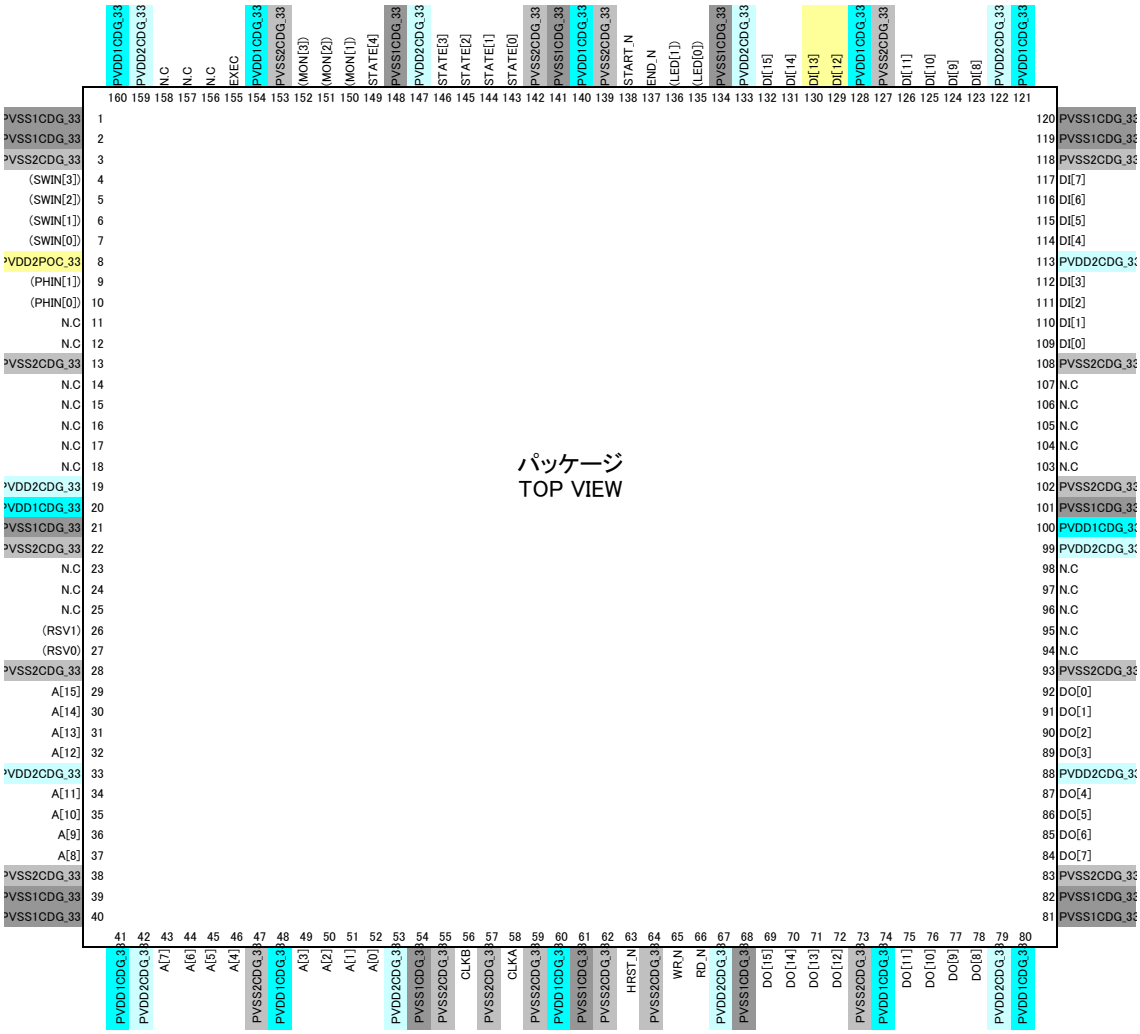


図 2.2　90nm 版暗号 LSI ピンアサインイメージ

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 2.4 に，データのリード/ライト/暗号処理のタイミングを図 2.3~2.5 に示す．このインタフェースレジスタを通じて下記の手順で，各暗号 IP コアの制御を行う．インタフェースレジスタの詳細は 3.3 節を参照のこと．

- AES5 以外の暗号アルゴリズムコア
  - ① 動作 IP 選択 ： IP 選択レジスタ(IPSEL0，1)の対応ビットをセット．
  - ② 選択 IP リセット ： CONT[IPRST]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(OUTSEL0，1)の対応ビットをセットする．
  - ④ 動作モード設定 ： モードレジスタ(MODE)を設定する．(*1)
  - ⑤ 鍵設定 ：
    - ⑤-1 共通鍵暗号は KEY0~7，RSA は EXP0~31 と MOD0~31，ECC は IDATA0~3 を設定する．
    - ⑤-2 CONT[KSET]をセットした後，同ビットがクリアされるまで待つ．
  - ⑥ 初期値(IV)設定 ： IV0~7 を設定する．(*2)
  - ⑦ 乱数(SEED)設定 ： RAND0~7 を設定する．(*3)

⑧ 暗号処理 ： (以下を繰り返す)
⑧-1 共通鍵暗号は ITEXT0~7(*4), RSA は IDATA0~31, ECC は IDATA8~13 を設定する.
⑧-2 CONT[RUN]をセットした後, 同ビットがクリアされるまで待つ.
⑧-3 共通鍵暗号は OTEXT0-7(*5), RSA は ODATA0~31, ECC は ODATA0~3 を読む.

(*1) AES6 を選択する場合は, 必要に応じてラウンド選択レジスタ(KRSEL, DRSEL)も設定する.
(*2) 初期値が必要な AES12, AES13 で設定する.
(*3) 乱数を使用する AES8, AES9, AES10 で設定する.
(*4) 64 ビットブロック暗号の場合は, ITEXT0~3 を設定する.
(*5) 64 ビットブロック暗号の場合は, OTEXT0~3 を読み出す.

なお、AES6 選択時は, ラウンド選択レジスタに設定したラウンドもしくは fault 発生時の中間値および中間鍵(ラウンド鍵)RDATA0~7/RKEY0~7 を読み出すことが可能である.

設定を変更は以下の手順で行う.

・暗号コアを変更する場合は, 上記①~⑧を改めて実行する.
・既に選択されている暗号コアの動作モード変更する場合は, 上記④~⑧を改めて実行する.
・既に選択されている暗号コアの鍵を変更する場合は, 上記⑤~⑧を改めて実行する.
・既に選択されている暗号コアの初期値を変更する場合は, 上記⑥~⑧を改めて実行する.
・既に選択されている暗号コアの乱数を変更する場合は, 上記⑦~⑧を改めて実行する.

● AES5(CTR モード+4 段パイプライン実装)
①~⑤ 上記の手順と同じ.
⑥ 初期値(IV)設定 ：
⑥-1 IV0-7 を設定する.
⑥-2 コントロールレジスタ CONT[RUN]に 1 を書き込み後, 同ビットがクリアされるのを待つ.
⑦ 乱数(SEED)設定 ：設定不要
⑧ 暗号処理 ： (以下を繰り返す)
⑧-1 ITEXT0~31 を設定する.
⑧-2 コントロールレジスタ CONT[RUN]に 1 を書き込み後, 同ビットがクリアされるのを待つ.
⑧-3 OTEXT0-31 を読み出す.

初期値を変更する場合は, 上記⑥~⑧を改めて実行する.

表 2.4 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	処理開始の指示(W)/終了の通知(R) 鍵生成の指示(W)/終了の通知(R) 暗号 IP のリセット制御(W)
		0004	IP 選択レジスタ 0	IPSEL0	R/W	動作させる暗号 IP を指定
		0006	IP 選択レジスタ1	IPSEL1	R/W	動作させる暗号 IP を指定
		0008	出力選択レジスタ 0	OUTSEL0	R/W	データ出力する暗号 IP を指定
		000A	出力選択レジスタ 1	OUTSEL1		データ出力する暗号 IP を指定
		000C	モードレジスタ	MODE	R/W	動作モード, 鍵長, 暗復号などを指定
		000E	ラウンド˝選択レジスタ	RSEL	R/W	中間値保存ラウンド˝数指定
		0010	テストレジスタ 1	TEST1	R/W	カスタムコア動作制御 1
		0012	テストレジスタ 2	TEST2	R/W	カスタムコア動作制御 2
		: 00FE	(予約)			
共通鍵暗号	秘密鍵(→LSI)	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)
	IV(→LSI)	0110	IV レジスタ 0	IV0	W	入力 IV(最上位 16 ﾋﾞｯﾄ)
		0112	IV レジスタ 1	IV1	W	入力 IV(IV0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		011E	IV レジスタ 7	IV7	W	入力 IV(最下位 16 ﾋﾞｯﾄ)
	入力テキスト(→LSI)	0120	入力ﾃｷｽﾄﾚｼﾞｽﾀ 0	ITEXT0	W	入力テキスト(最上位 16 ﾋﾞｯﾄ)
		0122	入力ﾃｷｽﾄﾚｼﾞｽﾀ 1	ITEXT1	W	入力テキスト(ITEXT0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		015E	入力ﾃｷｽﾄﾚｼﾞｽﾀ 31	ITEXT31	W	入力テキスト(最下位 16 ﾋﾞｯﾄ)
	乱数(→LSI)	0160	乱数レジスタ 0	RAND0	W	入力乱数(最上位 16 ﾋﾞｯﾄ)
		0162	乱数レジスタ 1	RAND1	W	入力乱数(RAND0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		016E	乱数レジスタ 7	RAND7	W	入力乱数(最下位 16 ﾋﾞｯﾄ)
	(予約)	: 017E	(予約)			
	出力テキスト(←LSI)	0180	出力ﾃｷｽﾄﾚｼﾞｽﾀ 0	OTEXT0	R	出力テキスト(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(OTEXT0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		01BE	出力ﾃｷｽﾄﾚｼﾞｽﾀ 31	OTEXT31	R	出力テキスト(最下位 16 ﾋﾞｯﾄ)
	中間値データ(←LSI)	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	中間値データ(最下位 16 ﾋﾞｯﾄ)
	中間鍵(←LSI)	01D0	中間鍵レジスタ 0	RKEY0	R	中間鍵(最上位 16 ﾋﾞｯﾄ)
		01D2	中間鍵レジスタ 1	RKEY1	R	中間鍵(RKEY0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		01DE	中間鍵レジスタ 7	RKEY7	R	中間鍵(最下位 16 ﾋﾞｯﾄ)
	(予約)	: 01FE	(予約)			

表 2.4 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・鍵(←LSI)	0200	指数レジスタ 0	EXP0	W	指数(最上位 16 ﾋﾞｯﾄ)
		0202	指数レジスタ 1	EXP1	W	指数(EXP0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		023E	指数レジスタ 31	EXP31	W	指数(最下位 16 ﾋﾞｯﾄ)
		: 02FE	(予約)			
	法(→LSI)	0300	法レジスタ 0	MOD0	W	法(最上位 16 ﾋﾞｯﾄ)
		0302	法レジスタ 1	MOD1	W	法(MOD0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		033E	法レジスタ 31	MOD31	W	法(最下位 16 ﾋﾞｯﾄ)
	前処理演算結果入力(→LSI)	0340	前処理結果ﾚｼﾞｽﾀ 0	PREDAT0	W	前処理演算結果(最上位 16 ﾋﾞｯﾄ)
		0342	前処理結果ﾚｼﾞｽﾀ 1	PREDAT1	W	前処理演算結果(PREDAT0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		035E	前処理結果ﾚｼﾞｽﾀ 15	PREDAT15	W	前処理演算結果(最下位 16 ﾋﾞｯﾄ)
		: 03FE	(予約)			
	入力データ(→LSI)	0400	入力ﾃﾞｰﾀﾚｼﾞｽﾀ 0	IDATA0	W	入力データ(最上位 16 ﾋﾞｯﾄ)
		0402	入力ﾃﾞｰﾀﾚｼﾞｽﾀ 1	IDATA1	W	入力データ(IDATA0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		043E	入力ﾃﾞｰﾀﾚｼﾞｽﾀ 31	IDATA31	W	入力データ(最下位 16 ﾋﾞｯﾄ)
		: 04FE	(予約)			
	出力データ(←LSI)	0500	出力ﾃﾞｰﾀﾚｼﾞｽﾀ 0	ODATA0	R	出力データ(最上位 16 ﾋﾞｯﾄ)
		0502	出力ﾃﾞｰﾀﾚｼﾞｽﾀ 1	ODATA1	R	出力データ(ODATA0 に続く 16 ﾋﾞｯﾄ)
		:	:	:	:	:
		053E	出力ﾃﾞｰﾀﾚｼﾞｽﾀ 31	ODATA31	R	出力データ(最下位 16 ﾋﾞｯﾄ)
		: 05FE	(予約)			
(空き)		0600 : FFEE				
LSI 情報 (0xFFF0 ～0xFFFF)		FFF0 :	(予約)			
		FFFC	バージョンレジスタ	VER	R	
		FFFE	(予約)		--	

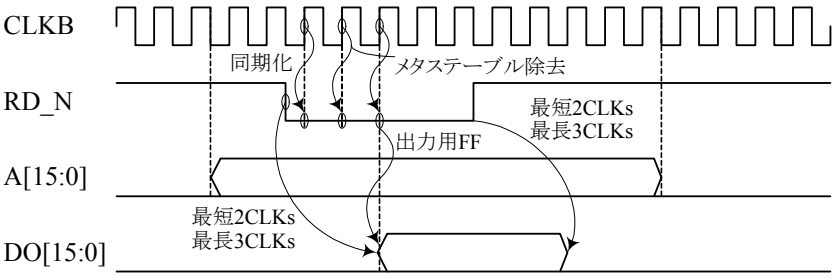


図 2.3 リードサイクルのタイミングチャート

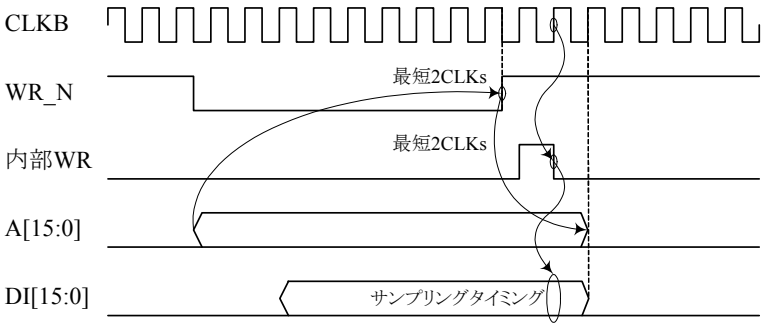
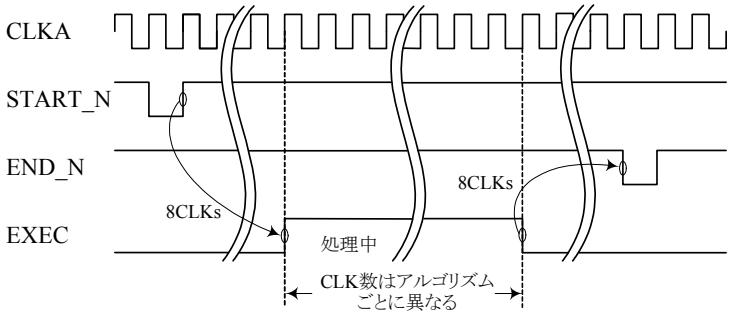


図 2.4 ライトサイクルのタイミングチャート



START_N:アルゴリズムの処理開始信号(Active “L”)
END_N:アルゴリズムの処理終了信号(Active “L”)
EXEC;アルゴリズムの演算実行中(Active “H”)

図 2.5 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 3.1 に, また各暗号 IP のソースコードの階層構造を図 3.2 に示す. 暗号 LSI は表 3.1 の 22 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.

表 3.1 暗号 IP コア

IP No.	IP コア	HDL ソース Top モジュール	内容
1	AES0 (合成体 S-box)	AES_Comp	合成体の 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.
2	AES1 (テーブル S-box)	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	AES2 (1-stage PPRM S-box)	AES_PPRM1	Positive Prime Reed-Muler (PPRM)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	AES3 (3-stage PPRM S-box)	AES_PPRM3	PPRM 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	AES4 (合成体 S-box)	AES_Comp_ENC_top	AES_Comp の暗号化部のみの実装.
6	AES5 (CTR モード)	AES_CTR_PIPE	4 段のパイプライン実装を行った AES コアにより CTR モードをサポート. S-box は合成体を使用.
7	AES6 (FA 対策済)	AES_FA	誤動作による内部データのエラー検出を行う機構を備えた, 故障利用解析攻撃(FA: Fault injection Attack)対策を実装. 暗号化と復号をサポート. S-box は合成体を使用.
8	AES7 (ラウンド鍵事前生成)	AES_PKG	11 個のラウンド鍵を事前生成し, レジスタファイルに保存する実装.
9	AES8 (MAO)	U_YNU_MA_AESTOP	DPA 対策として Masked And Operation (MAO)を施した実装
10	AES9 (MDPL)	U_YNU_ML_AESTOP	DPA 対策として Masked Dual-rail Precharge Logic (MDPL)を施した実装
11	AES10 (Threshold)	U_YNU_TI_AESTOP	DPA 対策として Threshold implementayion を施した実装
12	AES11 (WDDL)	U_YNU_WL_AESTOP	DPA 対策として Wave Dynamic Differential Logic (WDDL)を施した実装
13	AES12 (疑似 RSL)	JIP_PR_AESTOP	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.
14	AES13 (疑似 RSL)	JIP_WO_AESTOP	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.

15	Camellia	Camellia	128 ビットブロック暗号 Camellia. S-box は case 文で記述.
16	CAST-128	CAST128	128 ビット鍵による 64 ビットブロック暗号 CAST128.
17	DES	DES	56 ビット鍵による 64 ビットブロック暗号の Single DES.
18	ECC	Uec_ECC_OS	GF(2^{61})上の楕円曲線のスカラー倍算
19	MISTY1	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.
20	RSA	RSA	32 ビット乗算器による Montgomery 乗算を用いた RSA 暗号.
21	SEED	SEED	128 ビット鍵による 64 ビットブロック暗号 SEED.
22	TDES	TDEA	3-key Triple DES

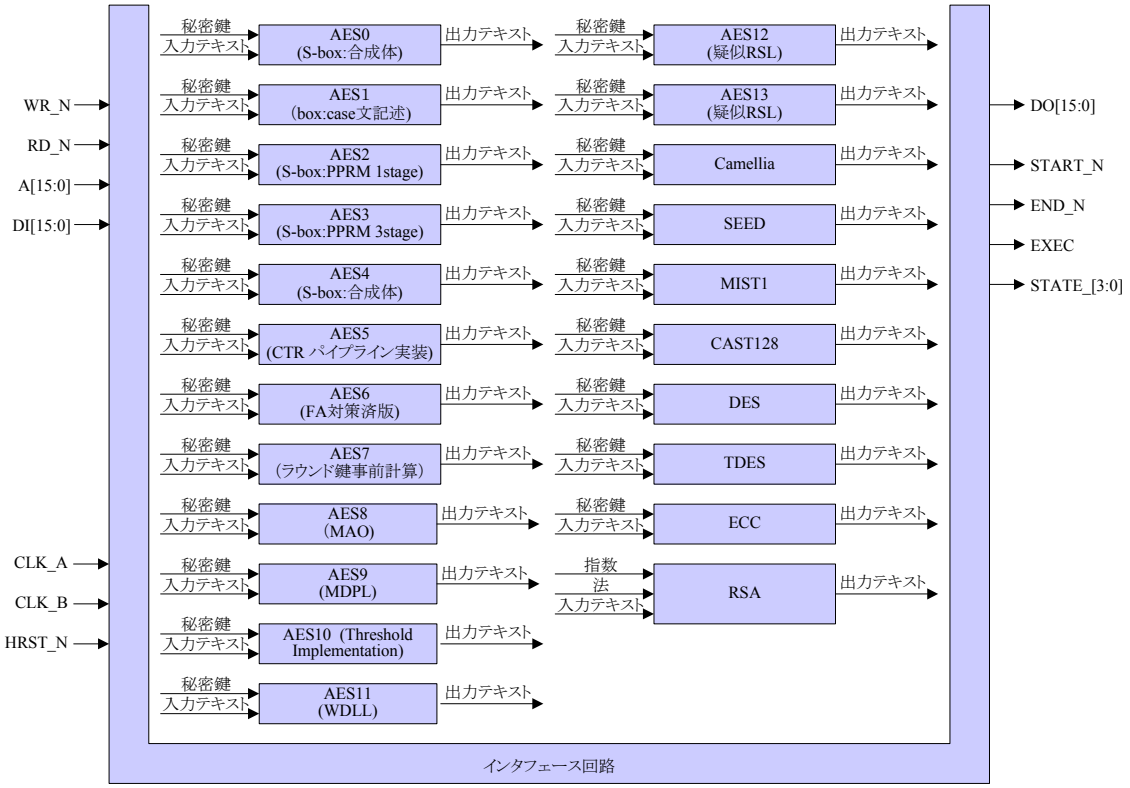


図 3.1 全体ブロック図

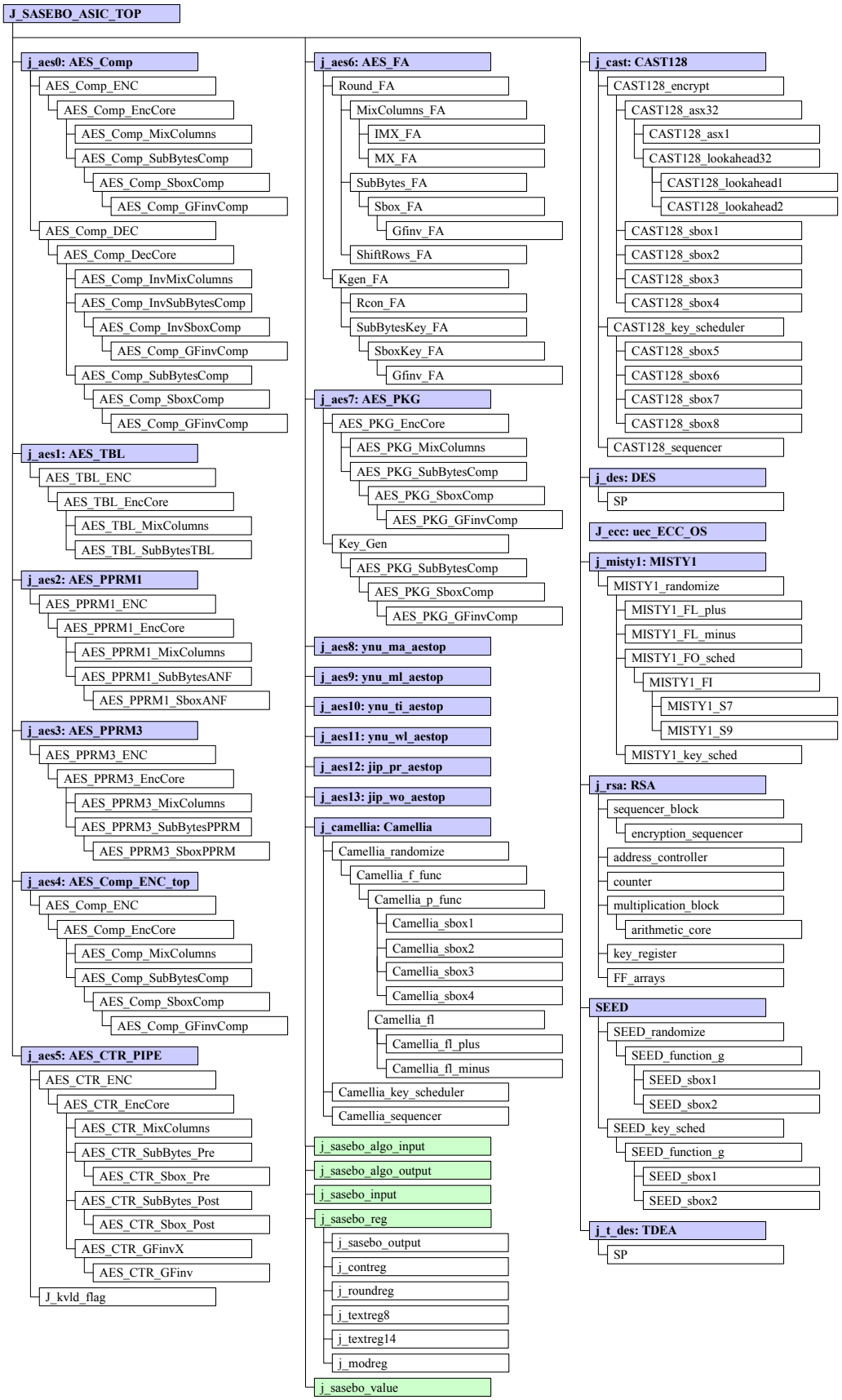
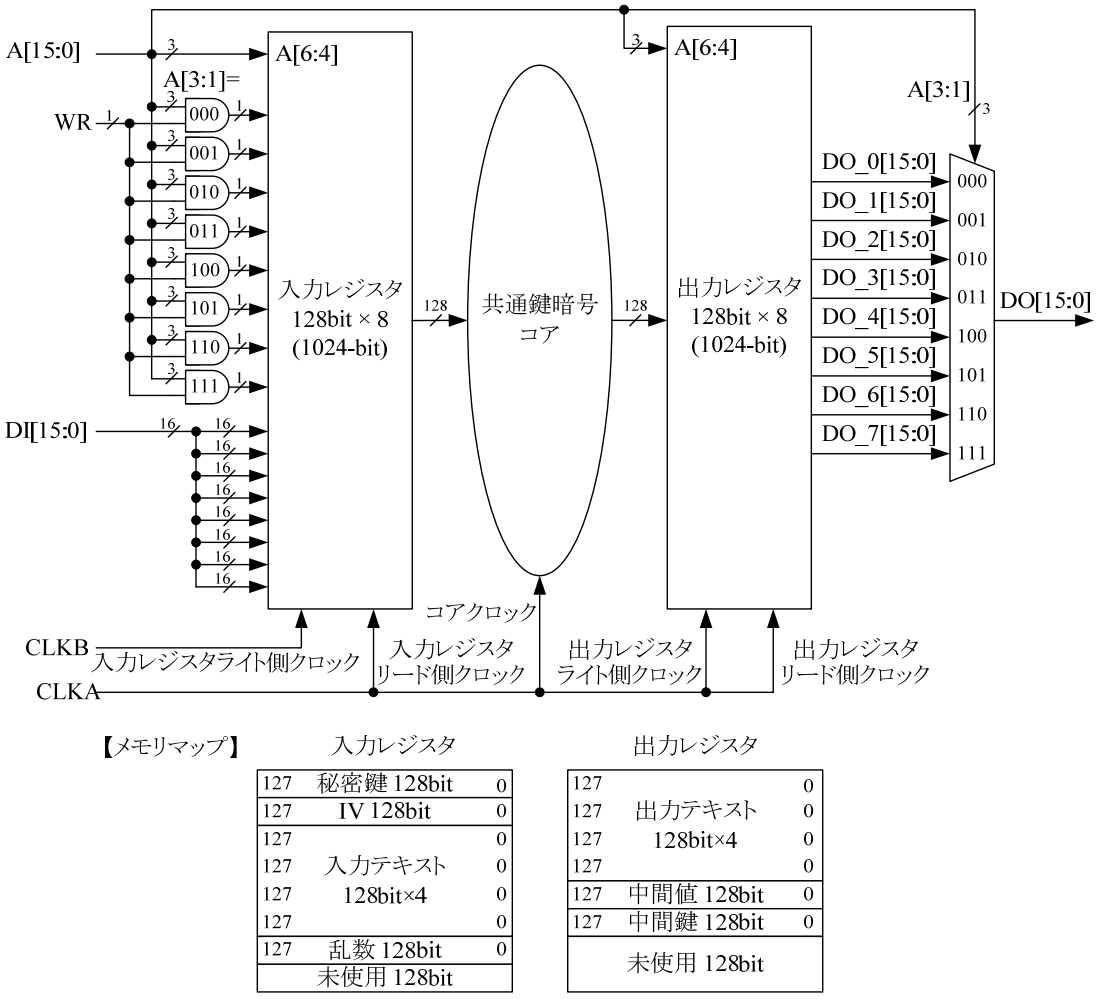

J_SASEBO_ASIC_TOP
j_aes0: AES_Comp
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColumns
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
AES_Comp_DEC
AES_Comp_DecCore
AES_Comp_InvMixColumns
AES_Comp_InvSubBytesComp
AES_Comp_InvSboxComp
AES_Comp_GFinvComp
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
j_aes1: AES_TBL
AES_TBL_ENC
AES_TBL_EncCore
AES_TBL_MixColumns
AES_TBL_SubBytesTBL
j_aes2: AES_PPRM1
AES_PPRM1_ENC
AES_PPRM1_EncCore
AES_PPRM1_MixColumns
AES_PPRM1_SubBytesANF
AES_PPRM1_SboxANF
j_aes3: AES_PPRM3
AES_PPRM3_ENC
AES_PPRM3_EncCore
AES_PPRM3_MixColumns
AES_PPRM3_SubBytesPPRM
AES_PPRM3_SboxPPRM
j_aes4: AES_Comp_ENC_top
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColumns
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
j_aes5: AES_CTR_PIPE
AES_CTR_ENC
AES_CTR_EncCore
AES_CTR_MixColumns
AES_CTR_SubBytes_Pre
AES_CTR_Sbox_Pre
AES_CTR_SubBytes_Post
AES_CTR_Sbox_Post
AES_CTR_GFinvX
AES_CTR_GFinv
J_kvld_flag
j_aes6: AES_FA
Round_FA
MixColumns_FA
IMX_FA
MX_FA
SubBytes_FA
Sbox_FA
Gfinv_FA
ShiftRows_FA
Kgen_FA
Rcon_FA
SubBytesKey_FA
SboxKey_FA
Gfinv_FA
j_aes7: AES_PKG
AES_PKG_EncCore
AES_PKG_MixColumns
AES_PKG_SubBytesComp
AES_PKG_SboxComp
AES_PKG_GFinvComp
Key_Gen
AES_PKG_SubBytesComp
AES_PKG_SboxComp
AES_PKG_GFinvComp
j_aes8: ynu_ma_aestop
j_aes9: ynu_ml_aestop
j_aes10: ynu_ti_aestop
j_aes11: ynu_wl_aestop
j_aes12: jip_pr_aestop
j_aes13: jip_wo_aestop
j_camellia: 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
j_sasebo_algo_input
j_sasebo_algo_output
j_sasebo_input
j_sasebo_reg
j_sasebo_output
j_contreg
j_roundreg
j_textreg8
j_textreg14
j_modreg
j_sasebo_value
j_cast: 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
j_des: DES
SP
J_ecc: uec_ECC_OS
j_misty1: MISTY1
MISTY1_randomize
MISTY1_FL_plus
MISTY1_FL_minus
MISTY1_FO_sched
MISTY1_FI
MISTY1_S7
MISTY1_S9
MISTY1_key_sched
j_rsa: RSA
sequencer_block
encryption_sequencer
address_controller
counter
multiplication_block
arithmetic_core
key_register
FF_arrays
SEED
SEED_randomize
SEED_function_g
SEED_sbox1
SEED_sbox2
SEED_key_sched
SEED_function_g
SEED_sbox1
SEED_sbox2
j_t_des: TDEA
SP

図 3.2 階層構造

3.2 外部インタフェース回路

図 3.3 に共通鍵暗号(AES, DES, MISTY1, Camellia, SEED, CAST128), 図 3.4 に公開鍵暗号(RSA, ECC)の外部インタフェース回路を示す.



【メモリマップ】

入力レジスタ

127	秘密鍵 128bit	0
127	IV 128bit	0
127		0
127	入力テキスト	0
127	128bit×4	0
127		0
127	乱数 128bit	0
	未使用 128bit	

出力レジスタ

127		0
127	出力テキスト	0
127	128bit×4	0
127		0
127	中間値 128bit	0
127	中間鍵 128bit	0
	未使用 128bit	

図 3.3 共通鍵暗号アルゴリズムのインタフェース回路

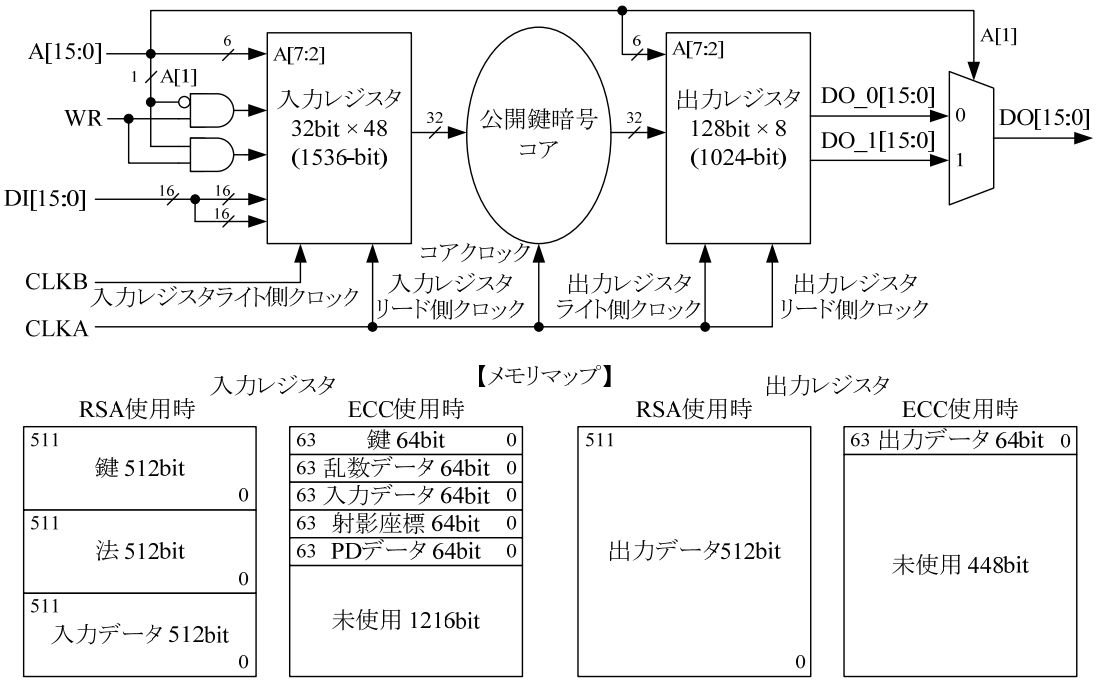


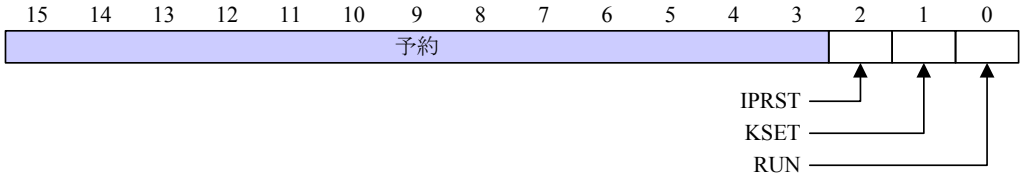
図 3.4　公開鍵暗号のインタフェース回路

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 が動作を開始する. 内部処理では, RUNビットの情報はインてフェースクロックCLKBから内部クロックCLKAへ同期化した後, CLKA において 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

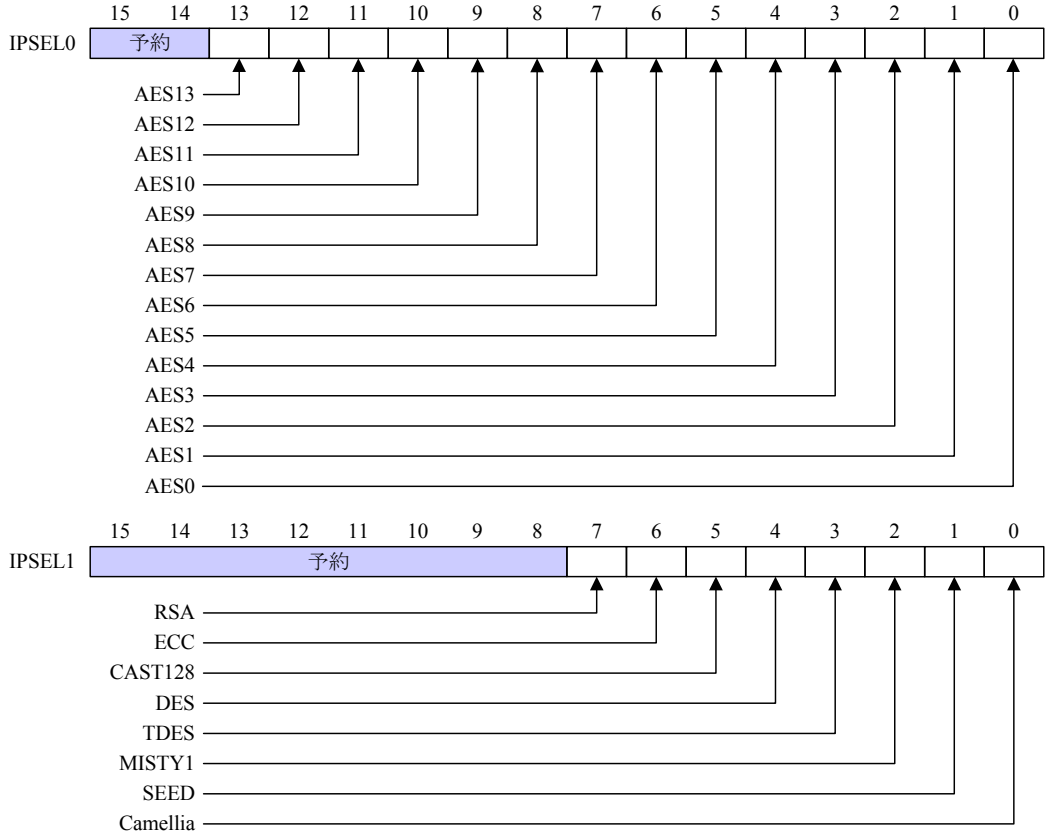
1 を書き込むことで, IP 選択レジスタ(IPSEL)で指定した暗号 IP に, モードレジスタ MODE に応じた鍵生成(鍵設定)が行われる. 出力選択レジスタ(OUTSEL)で指定した暗号 IP の鍵生成(鍵設定)が終了し, 設定された鍵を用いた暗号処理が可能になると, 本ビットは自動的に 0 クリアされる. 本ビットが 1 の期間中は, 全てのレジスタへの書き込みは原則禁止とする. 特に, 本ビットが 1 の期間中に RUN ビットをセットした場合の動作は保証されない.

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．

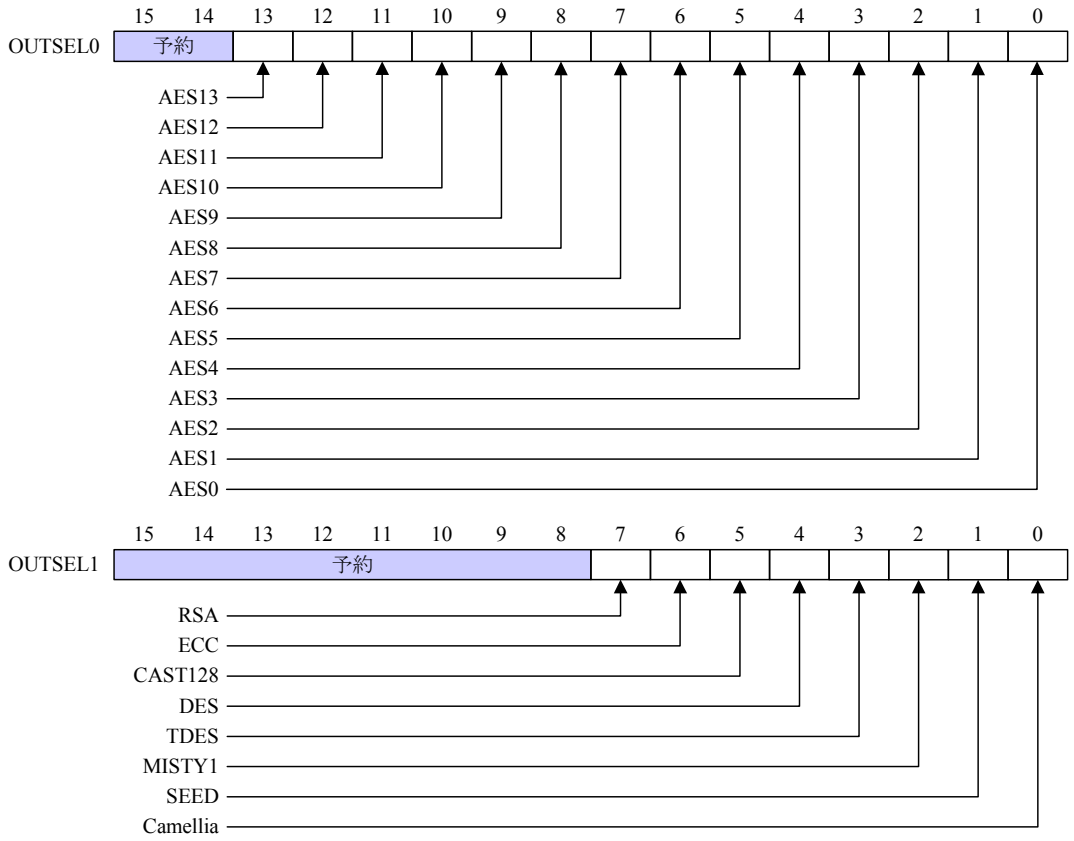
- **IP 選択レジスタ : IPSEL**

22 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だけが active 状態となり，選択 IP 以外にはクロックは供給されない．



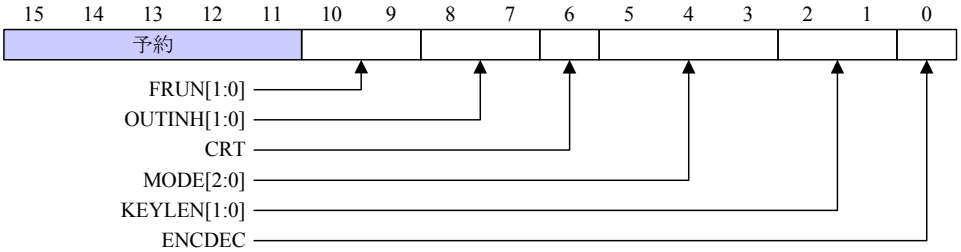
- **出力選択レジスタ : OUTSEL**

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 10-9：FRUN

AES0 のみがサポートする 0.3 秒に 1 回自動実行するフリーランモード制御

FRUN[1]：	0	フリーランモードモード OFF
	1	フリーランモードモード ON
FRUN[0]：	0	ITEXT を初期値に+1 インクリメントしながらフリーラン
	1	ITEXT を初期値に暗号化結果を次回入力にしながらフリーラン

Bit 8-7：OUTINH

制御信号の出力抑止制御

OUTINH[1]：	0	制御信号出力抑止機能 OFF(制御信号は出力される)
	1	制御信号出力抑止機能 ON(内容は OUTINH[0]による)
OUTINH[0]：	0	全ての制御信号出力を抑止
	1	START 信号を除く制御信号出力を抑止

Bit 6：CRT

RSA 以外の IO では意味を持たない．本ビットは RSA コアの CRT ポートに直結される．なお現在の LSI の CRT モードはデータによっては正しく動作しないバグが存在する．

0：CRT 処理 OFF

1：CRT 処理 ON

Bit 5-3：MODE[2:0]

RSA 利用時にはこのビットが RSA の MODE 入力に直結し，値に応じて下記の処理を行う．ECC コアにも 3 ビットの動作モード制御ビットがあるが，インタフェース回路では 3'b000 に固定してあり，この MODE ビットは仕使用されない．共通鍵暗号に対する動作モードは，AES12 がレジスタ TEST2(仕様非公開)を利用し，それ以外の暗号マクロの暗号利用モードまたは動作モードは IP 毎に固定されている．

000：左バイナリ法

001：右バイナリ法

010：対策版左バイナリ

011：対策版右バイナリ法

100：Montgomery Powering Ladder

101：M.Joye の右バイナリ法

Bit 2-1：KEYLEN[1:0]

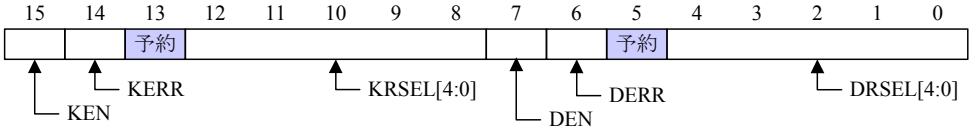
値は 00 に固定されており，IP 毎に決まっている鍵長が用いられる．

Bit 0：ENCDEC

0 で暗号化，1 で復号を行う．暗号化のみの IP が選択された場合，このビットは意味を持たない．

- **ラウンド選択レジスタ：RSEL**

中間値レジスタ(RDATA0~7)および中間鍵レジスタ(RKEY0~7)に値を取り込むラウンド数を指定する．DRSEL，RDATA0~7 および KRSEL，RKEY0~7 は，active な暗号 IP として故障利用解析攻撃対策が施された AES6 が選択されているときだけ意味を持つ．



Bit 15：KEN

0: 中間鍵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: 中間鍵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 14：KERR：鍵データエラーステータス(AES_FA の Err[0]に直結)

0: 正常動作

1: エラー発生

Bit 12~8：KRSEL[4:0]

中間鍵レジスタ（RKEY0~7）に中間鍵データを格納すべきラウンド数．

Bit 7：DEN

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）．

Bit6：DERR

データエラーステータス(AES_FA の Err[1]に直結)

0: 正常動作

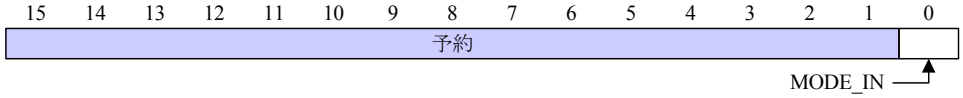
1: エラー発生

Bit 4~0：DRSEL[4:0]

中間値レジスタ（RDATA0~7）に中間値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 TEST1 の Bit0 に 1 をセットすることで，外部から入力した鍵の代わりに内部鍵(非公開)を使用した暗号化が行われる．一度 TEST1 がセットされると，外部からの入力鍵を使用する通常の暗号処理に戻るためには，電源を落とすかハードウェアリセット HRST_N をかける必要がある．このモードは 14 種類の全ての AES 暗号 IP コアがサポートしている．



- **テストレジスタ 2：TEST2**

テストレジスタ TEST2 は疑似 RSL 対策版 AES コア AES12 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 KEY0~7 は，16bit×8=128bit 分用意されているが，輸出規制の関係から KEY4 の下位 8bit と，KEY5~7 の合計 56bit 分だけを使用する．各暗号コアの鍵の取り扱いは次の通り．

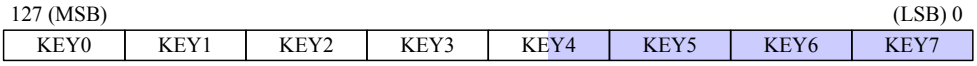
DES： パリティビットを除いた 56bit の鍵を KEY4 の下位 8bit 及び KEY5~7 に入力する．DES 暗号コアはこの 56bit の鍵に対して回路中で，パリティビットを付加して 64 ビットとしている．

TDES： パリティビットを除いた 56bit の鍵を KEY4 の下位 8bit 及び KEY5~7 に入力する．T-DES 暗号コアには，鍵は以下のように入力される．

[191:64] : 0x000102030405060708090a0b0c0d0e0f （固定値）
[63:0] : ユーザが入力した 56bit の鍵にパリティを追加したもの

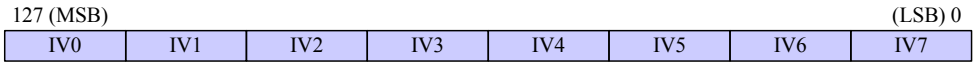
その他： アルゴリズムの鍵長が 128bit であるため，上位 72 ビットを以下のように固定し，KEY4 の下位 8bit 及び KEY5~7 の 56 ビットをユーザが設定する．

[127:56] : 0x000102030405060708
[55:0] : ユーザが入力した鍵



- **GCM モード用 IV レジスタ：IV0~7**

AES5 がサポートする GCM モードで使用する 128bit のイニシャルベクタ IV をセットする．



- **共通鍵暗号用入力テキストレジスタ：ITEXT0~31**

入力テキストレジスタは，IP 選択レジスタ：IPSEL で指定される IP が使用する入力テキストを保持する．各暗号コアにより以下のようにデータサイズ，使用する入力テキストレジスタの場所が異なるので注意が必要である．

AES5(AES_CTR_PIPE)： 128bit×4 ブロック分入力する．
ITEXT0~7 128bit 1 ブロック目入力
ITEXT8~15 128bit 2 ブロック目入力
ITEXT16~23 128bit 3 ブロック目入力

ITEXT24~31　　128bit　4 ブロック目入力
64bit ブロック暗号群(MISTY1, TDES, DES, CAST128)
ITEXT0~3　　64bit 入力
ITEXT4~31　　未使用
128bit ブロック暗号群
ITEXT0~7　　128bit 入力
ITEXT8~31　　未使用

127 (MSB) (LSB) 0

ITEXT0	ITEXT1	ITEXT2	ITEXT3	ITEXT4	ITEXT5	ITEXT6	ITEX7
ITEXT8	ITEXT9	ITEXT10	ITEXT11	ITEXT12	ITEXT13	ITEXT14	ITEX15
ITEXT16	ITEXT17	ITEXT18	ITEXT19	ITEXT20	ITEXT21	ITEXT22	ITEX23
ITEXT24	ITEXT25	ITEXT26	ITEXT27	ITEXT28	ITEXT29	ITEXT30	ITEX31

- **乱数レジスタ：RAND0~7**

サイドチャネル攻撃対策を施した暗号コア AES8, AES9, AES10 において使用される乱数の SEED をセットする. 1 度乱数レジスタに SEED が入力されると, 暗号化処理の度にレジスタは新たな乱数で自動的似更新される. AES9 の乱数は, 32bit であるため, SEED は上位側 RAND0~1 に詰めて入力する.

127 (MSB) (LSB) 0

RAND0	RAND1	RAND2	RAND3	RAND4	RAND5	RAND6	RAND7

- **共通鍵暗号用出力テキストレジスタ:OTEXT0~31**

出力テキストレジスタは, 出力選択レジスタ OUTSEL で選択されている IP の出力テキストを保持する. 各暗号コアにより以下のように出力データサイズ, 出力先のレジスタが異なるので注意が必要である.

また AES5 の仕様は他の暗号コアと異なり, 入出力とも連続データした 128bit×4 ブロック単位で処理が行われる. IV レジスタにデータを入力すると, CTR モードの乱数生成部分の処理だけが行われ, 出力テキストレジスタ OTEXT へはデータは出力されない. それに続いて入力テキストレジスタ ITEXT へデータがセットされると, 暗号化処理(前回生成した乱数と入力テキストとの XOR)が行われて OUTEXT へデータが出力されるとともに, 次の入力テキストに対して使用される乱数生成が行われる.

AES5(AES_CTR_PIPE):　　128bit×4 ブロック分出力される.
OTEXT0~7　　128bit　1 ブロック目入力
OTEXT8~15　　128bit　2 ブロック目入力
OTEXT16~23　　128bit　3 ブロック目入力
OTEXT24~31　　128bit　4 ブロック目入力
64bit ブロック暗号群(MISTY1, TDES, DES, CAST128)
OTXT0~3　　64bit 出力
OTEXT4~7　　0x0000000000000000
OTXT8~31　　未使用
128bit ブロック暗号群
OTEXT0~7　　128bit 出力
OTEXT8~31　　未使用

127 (MSB) (LSB) 0

OTEXT0	OTEXT1	OTEXT2	OTEXT3	OTEXT4	OTEXT5	OTEXT6	OTEX7
OTEXT8	OTEXT9	OTEXT10	OTEXT11	OTEXT12	OTEXT13	OTEXT14	OTEX15
OTEXT16	OTEXT17	OTEXT18	OTEXT19	OTEXT20	OTEXT21	OTEXT22	OTEX23
OTEXT24	OTEXT25	OTEXT26	OTEXT27	OTEXT28	OTEXT29	OTEXT30	OTEX31

- **共通鍵暗号用中間値レジスタ:RDATA0~7**

AES6 実行時の各ラウンドの中間値の読み出しのためのレジスタ群で，IP 選択レジスタ IPSEL/OUTSEL で AES6 が選ばれ，かつ，ラウンド選択レジスタ RSEL の DEN ビットを'1'にした場合に有効となる．中間値の保持は以下の 2 つのケースについて実行される．なお，中間値出力機能の使用時でも暗号化・復号処理は最後まで継続し，その最終結果が出力テキストレジスタ OTEXT に保持される．

1. 中間値を保持するラウンドを指定する場合
   ラウンド選択レジスタ:RSEL[DRSEL]で示されるラウンドの中間値が保持され，データの並びは RDA]TA0 に最上位 16 ビット分のデータ，以下 RDATA1，RDATA2…と続く．
2. Fault Error 発生時
   ラウンド処理中，途中結果に Fault Error が発生した際には(AES6 のモジュール AES_FA でエラー検出信号が Err[0]=1 にアサートされる)，ラウンド選択レジスタ RSEL の DERR がアサートされると共に，そのときの中間値が保持される．

127 (MSB) (LSB) 0

RDATA0	RDATA1	RDATA2	RSATA3	RDATA4	RDATA5	RDATA6	RDATA7

- **共通鍵暗号用中間鍵レジスタ:RKEY0~7**

AES6 実行時の各ラウンドの中間鍵の読み出しのためのレジスタ群で，IP 選択レジスタ IPSEL/OUTSEL で AES6 が選ばれ，かつ，ラウンド選択レジスタ RSEL の KEN ビットを'1'にした場合に有効となる．中間鍵の保持は以下の 2 つのケースについて実行される．なお，中間鍵出力機能の使用時でも暗号化・復号処理は最後まで継続し，その最終結果が出力テキストレジスタ OTEXT に保持される．

1. 中間鍵を保持するラウンドを指定する場合
   ラウンド選択レジスタ:RSEL[KRSEL]で示されるラウンドの中間鍵が保持され，データの並びは RKEY0 に最上位 16 ビット分のデータ，以下 RKEY1，RKEY2…と続く．
2. Fault Error 発生時
   ラウンド処理中，途中結果に Fault Error が発生した際には(AES6 のモジュール AES_FA でエラー検出信号が Err[0]=1 にアサートされる)，ラウンド選択レジスタ RSEL の DERR がアサートされると共に，そのときの中間鍵が保持される．中間鍵にエラーがあっても，それは全ラウンドの処理が終了するまで判定することができない（AES_FA でエラー検出信号が Err[1]=1 にアサートされるのは最終ラウンド終了時に限られる）．したがって KERR はラウンド処理途中でアサートされることはなく，最終ラウンド処理後となる．このため中間鍵レジスタは，“途中結果”にエラーが生じたときの中間鍵を保存する目的に使用される．逆に，中間鍵にエラーがあってもどのラウンドかは分からないため，エラー発生時の途中結果は保存されれない．

127 (MSB) (LSB) 0

RKEY0	RKEY1	RKEY2	RKEY3	RKEY4	RKEY5	RKEY6	RKEY7

- **公開鍵暗号用指数レジスタ:EXP0~31**

RSA の 512 ビットの指数を入力する. EXP0 に最上位 16 ビット分の指数が保持され, 以下 EXP1, EXP2, …と続く. ECC では使用しない.

- **公開鍵暗号用法レジスタ:MOD0~31**

RSA の 512 ビットの法を入力する. MOD0 に最上位 16 ビット分の法が保持され, 以下 MOD1, MOD2, …と続く. ECC では使用しない.

- **公開鍵暗号用前処理演算結果レジスタ:PREDAT0~15**

RSA の CTR 処理時の 256 ビットの前処理演算結果を入力する. PREDAT0 に最上位 16 ビット分の指数が保持され, 以下 PREDAT1, PREDAT2, …と続く. ECC では使用しない.

- **公開鍵暗号用入力データレジスタ:IDATA0-31**

RSA では 512 ビットのデータ入力に使用され, IDATAP0 に最上位 16 ビット分の入力データが保持され, 以下 IDATA1, IDATA2, …と続く.

ECC では下記のデータを入力する.

IDATA0~3:64bit 秘密鍵データ
IDATA4~7: サイドチャネル対策用 64bit 乱数データ.
将来サポート予定であり, 今回の ECC コアでは使用されない.
IDATA8~11:入力点の Affine 座標における x 座標データ(64bit)
IDATA12~15:入力点の射影座標における z 座標データ(64bit)
IDATA16~19:楕円曲線パラメータ b(64it)
IDATA20~31:未使用

いずれも, 添字が若い側に上位のデータを入力する.

- **公開鍵暗号用出力データレジスタ:ODATA0~31**

RSA では 512 ビットの計算結果が出力される. ODATA0 に最上位 16 ビットの計算結果が保持され, 以下 ODATA1, ODATA2, …と続く.

ECC では ODATA0~3 に 64 ビットの計算結果が出力される. ODATA0 に最上位の計算結果が保持され, 以下 ODATA1, ODATA2, ODATA3 と続く. ODATA4～31 は未使用である.

- **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. 130nm 版は固定値 0x0450A, 90nm 版は固定値 0x34F9 が読み出される.

3.4 クロックツリー

暗号 LSI では，インタフェースレジスタの設定により，測定対象とするコアだけに動作クロックを供給する．一方，故障解析を容易に行なうため，インタフェース回路クロックとコアクロックとを分離し，コアクロックにのみノイズを印加できる構成としている．

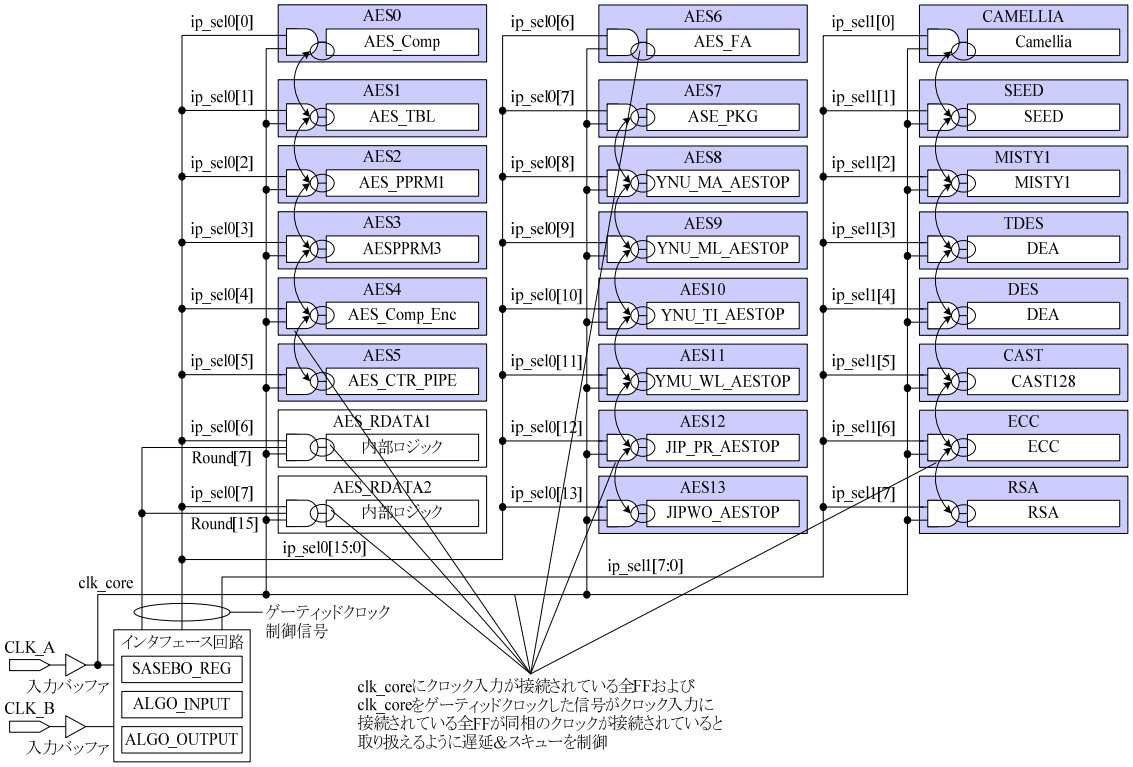


図 3.5 クロック系統図

3.5 リセット

図 3.6 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暗号 IP コア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. CLK_B 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，各暗号コア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 IP 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．

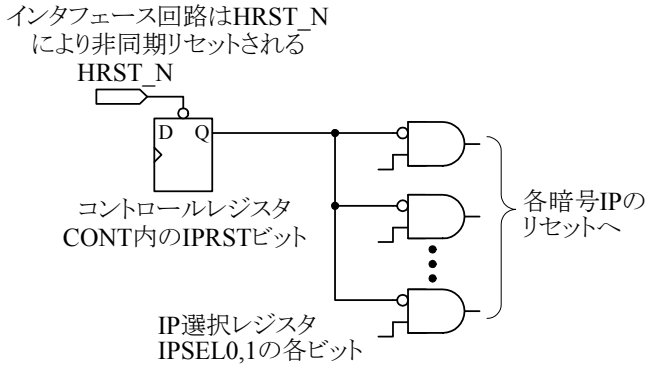


図 3.6 リセット系統

3.6 付帯機能

- **コアクロックとインタフェースクロック**

故障解析を容易にすることを目的に，コアのみに動作クロック由来の故障を印加するため，コアクロック CLK_A とインタフェースクロック CLK_B を分離している．そして，暗号 LSI 内同期化回路は簡略化のため，CLK_A と CLK_B の位相差は 180°（反転クロック）であることを前提とする設計を行なっている．

- **鍵長制限**

暗号 LSI は輸出管理対象とならないよう，共通鍵アルゴリズムの鍵長は 56 ビットに，RSA と ECC は 512 ビットと 64 ビットに制限されている．

DES はパリティビットを含まない 56 ビットの鍵を KEY4 の下位 8bit 及び KEY5~7 に入力する．DES の鍵データと暗号 LSI との対応を図 3.6 に示す．T-DES の上位[191:64]は以下の固定値がコアに供給される．下位[63:0]の扱いは DES と同じである．

[191:64]　0x000102030405060708090a0b0c0d0e0f (固定値)

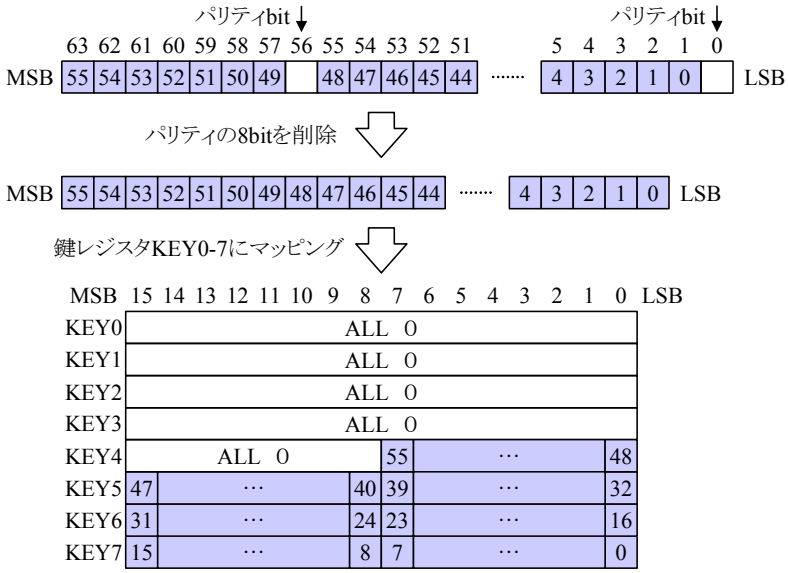


図 3.7　DES コア鍵データビットアサイン

その他共通鍵暗号アルゴリズムズムの鍵長は 128 ビットであるため，図 3.8 に示したように上位 72 ビットを固定値とし，下位 56 ビットだけをユーザが設定できるようにしている．

[127:56] 0x000102030405060708 (固定値)
[55:0] 入力された鍵 KEY4 下位 8 ビットと KEY5-7 を併せた 56 ビット

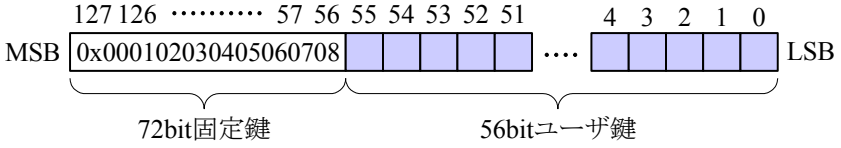


図 3.8 共通鍵データビットアサイン

- **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 8CLK 後に処理開始要求信号 START_N がアサートされ，さらにその 8CLK 後に暗号アルゴリズムコアが処理を開始して処理中であることを示す EXEC が High となる．アルゴリズムコアの処理終了により EXEC が Low に落ちると，その 8CLK 後に処理完了を示す END_N がアサートされる．更にその 8CLK 後にコントロールレジスタ CONT[RUN]が 0 となる．これら一連の動作の詳細を図 3.9 に示す．なお，CLK はいずれも CLK_A 換算である．

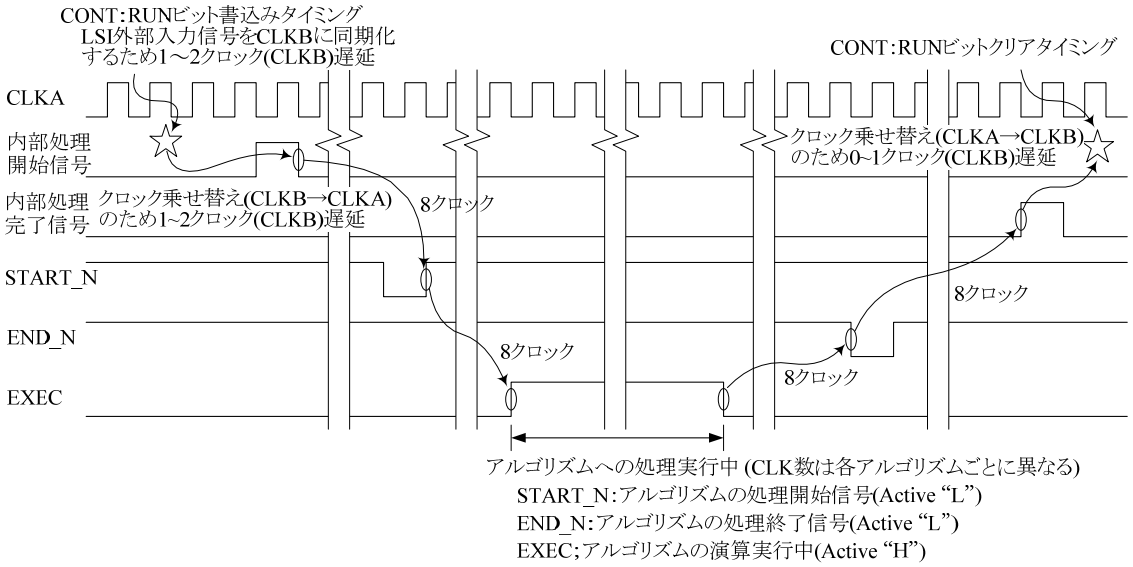


図 3.9 遅延実行のタイミングチャート

- ***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．

- **評価用信号の出力抑止機能**

電力波形や電磁波形測定時に制御回路のノイズ放射を低減するため，評価信号 START_N, END_N, EXEC, STATE の出力を抑止する次の 2 つの機能を設けている．

1. モードレジスタ MODE[OUTINH]を“10”に設定することで，全ての評価用信号出力を 0 にする．

2. MODE[OUTINH]を”11”に設定することで，START_N 以外の評価信号出力を 0 にする．

- **自走モード**

AES0 では，コントロールレジスタ CONT[RUN]を 1 にすることで，0.3 秒ごとに自動的に暗号化または復号処理を繰り返す自走モードでの動作が可能である．1 回目の処理が終了すると，コントロールレジスタ CONT[RUN]は 0 にリセットされ，そのまま 2 回目以降の処理が続行される．出力抑止機能を使用していない限り，START_N，EXEC，END_N は上記の遅延実行に応じて制御される．自走モードに入ると他の処理は実行できなくなり，自走モードの解除には，電源リセットかもしくは HRST_N をアサートする必要がある．なお，入力テキストは次の 2 つパターンから選択できる．

1. モードレジスタ MODE[FRUN]を “10” に設定することで，入力テキストレジスタ ITEXT にセットした平文または暗号文を初期値をとして，暗号化または復号処理が終わるごとに，自動的に+1 インクリメントを行う．
2. モードレジスタ MODE[FRUN]を “11” に設定することで，暗号化または復号処理完了時の暗号文または平文を，次の処理の入力とする．なお入力の初期値は，テキストレジスタ ITEXT にセットした平文または暗号文である．

- **入力テキストレジスタ ITEXT の取り扱い**

共通鍵暗号では以下に示すように，IP 毎に入力データサイズと入力テキストレジスタのマッピングが異なっているので注意が必要である．

1. AES5 (CTR モード+4 段パイプライン実装)
   - ITEXT0~7 128bit 入力 (1 ブロック目)
   - ITEXT8~15 128bit 入力 (2 ブロック目)
   - ITEXT16~23 128bit 入力 (3 ブロック目)
   - ITEXT24~31 128bit 入力 (4 ブロック目)
2. その他の 128 bit ブロック暗号
   - ITEXT0~7 128bit 入力
   - ITEXT8~31 未使用
3. 64bit ブロック暗号
   - ITEXT0~3 64bit 入力
   - ITEXT4~31 未使用

- **出力テキストレジスタ OTEXT の取り扱い**

共通鍵暗号では以下に示すように，IP 毎に出力データサイズと出力テキストレジスタのマッピングが異なっているので注意が必要である．

1. AES5 (CTR モード+4 段パイプライン実装)
   - OTEXT0~7 128bit 出力 (1 ブロック目)
   - OTEXT8~15 128bit 出力 (2 ブロック目)
   - OTEXT16~23 128bit 出力 (3 ブロック目)
   - OTEXT24~31 128bit 出力 (4 ブロック目)
2. その他の 128 bit ブロック暗号
   - OTEXT0~7 128bit 出力
   - OTEXT8~31 don't care
3. 64bit ブロック暗号
   - OTEXT0~3 64bit 出力
   - OTEXT4~7 0x0000000000000000
   - OTEXT8~31 don't care

- **DPA 対策用の乱数レジスタ RAND の取り扱い**

AES8(Masked AND Operation)、AES9(MDPL)、AES10(Threshold Implementation)で使用する初期乱数のシードを，乱数レジスタ RAND0~7 に入力するが，AES9 では乱数シードは 32bit でなのでレジスタの上位側が RAND0~1 だけが有効となる．

- **AES5(CTR モードサポートパイプライン)の CTR 動作について**

他の暗号コアと異なり，データ入出力は 128bit×4 ブロック連続して行われる．IV レジスタにカウンタの初期値を入力した直後には，CTR モード 4 ブロック分の乱数生成が行われるが，入力テキストレジスタ ITEXT に平文(または暗号文)が 4 ブロック入力されるまでは出力テキストレジスタ OTEXT からの出力はない．4 ブロックの暗号文(または平文)が出力されると，次の 4 ブロックの乱数生成が行われる．

- 中間値の出力

AES6(故障利用解析攻撃対策版)は中間値の出力が可能である．IP 選択レジスタ IPSEL0 および出力選択レジスタ OUTSEL0 で AES6 が選択され，かつラウンド選択レジスタ RSEL[DEN]が 1 の時に中間値レジスタ RDATA0~7 に中間値が出力される．なお，出力される中間値のラウンドは，ラウンド選択レジスタ RSEL[DRSEL]で決定する．

- 中間鍵の出力

AES6 は中間鍵(ラウンド鍵)の出力が可能である．IP 選択レジスタ IPSEL0 および出力選択レジスタ OUTSEL0 で AES6 が選択され，かつラウンド選択レジスタ RSEL[KEN]が 1 の時に中間鍵レジスタ RKEY0~7 に中間鍵が出力される．なお，出力されるラウンド鍵はラウンド選択レジスタ RSEL[KRSEL]で決定する．

- 故障利用解析攻撃(FA: Fault injection Attack)への対応

AES6 において，演算中に Fault Error が起きると，ラウンド選択レジスタの RSEL[KERR]あるいは RSEL[DERR]が 1 となり，その時の中間値とラウンド鍵がそれぞれ中間値レジスタ RDATA0~7 および中間鍵レジスタ RKEY0~7 に出力される．

4 LSI の物理レイアウト

4.1 130nm バージョン

130nm スタンダードセルライブラリを用いた暗号 LSI の論理合成後のレイアウト情報について述べる. 表 4.1 は LSI の概要で, 5×5 mm^2 のダイサイズのうち, 24.95%のゲートが使用されている. 目標の動作周波数は 24MHz (41ns cycle)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 4.1 暗号 LSI の概要

項目	
テクノロジ	0.13um Logic General Purpose 1P8M 1.2V-3.3V CU FSG
ウェハプロセス	TSMC CLN130G 130nm CMOS, アルミ 7 層配線
コア電源電圧	1.2±0.12V
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
セル使用数	4,129,178/16,550,023 (セル面積/セル配置可能面積)
セル使用率	24.95%
PAD 数	160 個
カスタムセル	SRAM

表 4.2 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	Z-2007.03-SP5
配置・配線	SOC Encounter	Cadence	v06.20-s285_1
RC 抽出	Star-RCXT	Synopsys	Z-2006.12-SP1
クロストーク抽出	CeltIC	Cadence	v06.20-s075_1
STA	PrimeTimeSI	Synopsys	Z-2007.06.-SP3
レイアウト検証	Calibre	Mentor	v2008.3-25.16
Power 検証	AstroRail	Synopsys	Z-2007.03-SP8
等価検証	Formality	Synopsys	Z-2007.06.SP-3

表 4.3 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	EZBond, I/O, TPZ013G3, 1.2V/3.3V	210c
RAM	2P-RF ADV(TSMC CL013G) FB	2004q2v1
	SP-RF ADV(TSMC CL013G) FB	2003q4v1

表 4.4 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	2ns
出力遅延	2ns
外部負荷容量	20pf
仮想配線遅延	tsmc130_w110

図 4.1 は暗号 LSI の電源ラインを除いた Top View を，図 4.2 はレジスタアレイの配置を，図 4.3 は各暗号モジュールの配置を示している．また，表 4.5 はそれらモジュールの回路規模の一覧である．また，表 2.11 は製造時のプロセスパラメータが Typical の場合において，動作環境が Worst (125℃ 1.08V)，Typical (25℃ 1.20V)，Best (-40℃ 1.32V)のときの LSI の動作速度であり，表 4.6 は各暗号モジュールの性能を示している．最も遅いモジュールはサイドチャネル攻撃対策の MDPL (Masked Dual-rail Precharge Logic)を用いた AES 回路で，Worst 条件において動作周波数 25.78 MHz（Typical: 41.24MHz, Best: 62.68MHz）で，回路規模も最大の 124,319 ゲートであった．ターゲットの 24MHz を達成しているが，表 4.6 より LSI 全体では Worst 条件において 20.410MHz (Typical: 24.889MHz, Best: 29.410MHz) と24MHz動作が達成されなかった．しかしながら，本LSIを実装する評価ボード SASEBO-R ではクロックを標準の 24MHz から変更可能であり，コア電圧も可変なため，実験において問題が生じることはない．

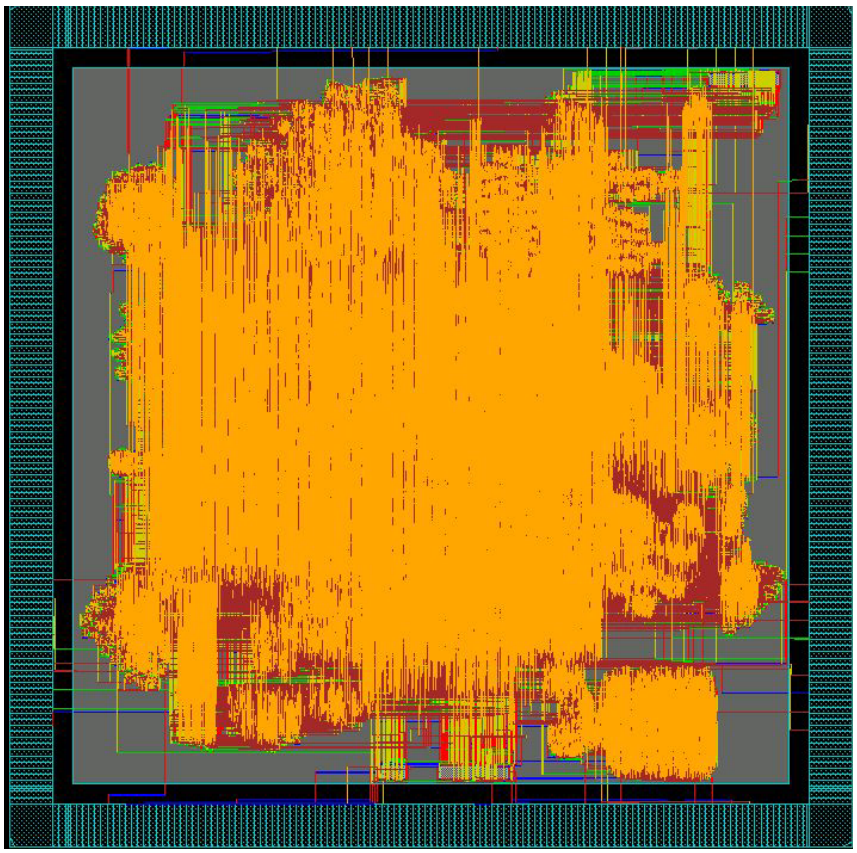


図 4.1 暗号 LSI の Top View

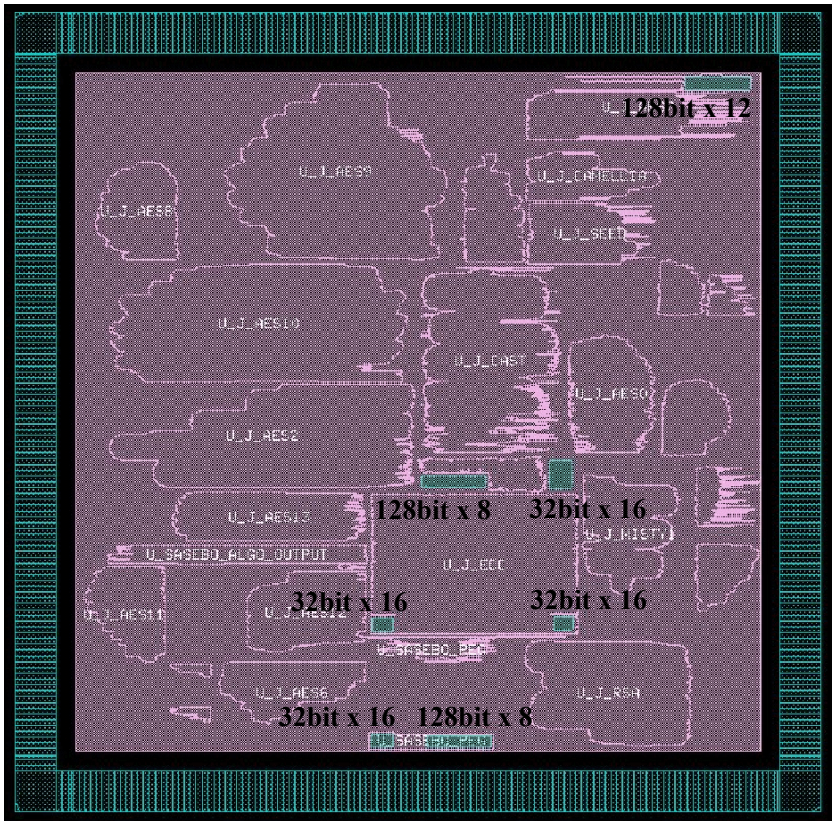


図 4.2　レジスタアレイ配置図

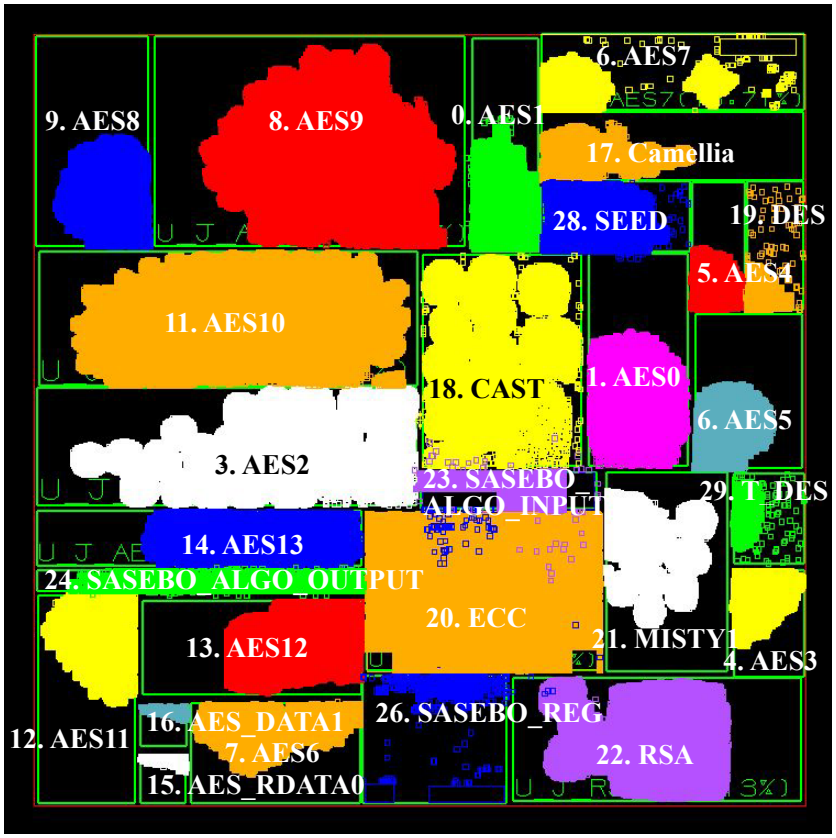


図4.3　暗号モジュール配置図

表 4.5 モジュール面積一覧

モジュール名	面積 (μm^2)	面積 (%)	ゲート数
1. AES0 (合成体 S-box)	129,763	2.7	25,483
2. AES1 (テーブル S-box)	105,097	2.2	20,639
3. AES2 (1-stage PPRM S-box)	314,702	6.5	61,801
4. AES3 (3-stage PPRM S-box)	84,230	1.7	16,541
5. AES4 (合成体 S-box)	61,408	1.3	12,059
6. AES5 (CTR モード)	112,794	2.3	22,150
7. AES6 (FA 対策済)	105,125	2.2	20,644
8. AES7 (ラウンド鍵事前生成)	93,655	1.9	18,392
9. AES8 (MAO)	179,253	3.7	35,202
10. AES9 (MDPL)	633,056	13.1	124,319
11. AES10 (Threshold)	555,510	11.5	109,090
12. AES11 (WDDL)	152,225	3.1	29,894
13. AES12 (疑似 RSL)	169,789	3.5	33,343
14. AES13 (疑似 RSL)	99,295	2.1	19,499
15. AES_RDATA2	7,373	0.2	1,448
16. AES_RDATA1	7,387	0.2	1,451
17. Camellia	73,407	1.5	14,416
18. CAST	148,921	3.1	29,245
19. DES	16,176	0.3	3,177
20. ECC	339,046	7.0	66,581
21. MISTY1	85,733	1.8	16,836
22. RSA	359,011	7.4	70,502
23. SASEBO_ALGO_INPUT	63,135	1.3	12,398
24. SASEBO_ALGO_OUTPUT	33,143	0.7	6,509
25. SASEBO_INPUT	2,400	0.0	471
26. SASEBO_REG	127,903	2.6	25,117
27. SASEBO_VALUE	596	0.0	117
28. SEED	115,237	2.4	22,630
29. T_DES	27,127	0.6	5,327
Total cell area	4,830,232	100.0	948,555

1 ゲート = 2 入力 NAND (3.69μm × 1.38μm)

表 4.6 Static Timing Analysis による LSI の動作速度

項目	Worst (125℃ 1.08V)	Typical (25℃ 1.2V)	Best (-40℃ 1.32V)
Maximum Frequency	20.410 MHz	24.889 MHz	29.410 MHz
Critical Path	48.995 ns	40.178 ns	33.993 ns
Hold Time	0.482 ns	0.340 ns	0.208 ns

表 4.7 Static Timing Analysis による各暗号モジュールの動作速度 (Typical プロセス時)

モジュール名	Worst (125℃ 0.9V)			Typical (25℃ 1.0V)			Best (-40℃ 1.1V)		
	Freq. (MHz)	Critic. (ns)	Hold (ns)	Freq (MHz)	Critic. (ns)	Hold (ns)	Freq (MHz)	Critic. (ns)	Hold (ns)
1. AES0 (合成体 S-box)	66.30	15.085	0.537	107.54	9.299	0.328	163.51	6.116	0.104
2. AES1 (テーブル S-box)	108.47	9.219	0.528	125.56	5.696	0.322	266.45	3.753	0.210
3. AES2 (1-stage PPRM S-box)	41.86	23.88	0.503	68.18	14.666	0.295	105.82	9.450	0.193
4. AES3 (3-stage PPRM S-box)	93.21	10.729	0.514	152.28	6.567	0.302	236.41	4.230	0.197
5. AES4 (合成体 S-box)	93.79	10.662	0.547	153.44	6.517	0.324	239.64	4.173	0.209
6. AES5 (CTR モード)	29.03	34.452	0.495	47.74	20.948	0.282	73.25	13.652	0.168
7. AES6 (FA 対策済)	46.41	21.546	0.516	74.35	13.449	0.324	111.91	8.936	0.209
8. AES7 (ラウンド鍵事前生成)	92.99	10.754	0.423	152.93	6.539	0.252	238.83	4.187	0.145
9. AES8 (MAO)	61.36	16.298	0.498	102.08	9.796	0.297	161.21	6.203	0.193
10. AES9 (MDPL)	25.78	38.786	0.431	41.24	24.249	0.241	62.68	15.955	0.147
11. AES10 (Threshold)	52.78	18.953	0.481	87.61	11.414	0.297	137.51	7.272	0.187
12. AES11 (WDDL)	54.00	18.517	0.393	88.33	22.323	0.216	135.01	7.407	0.128
13. AES12 (疑似 RSL)	30.36	32.940	0.319	35.51	28.164	0.197	39.14	15.499	0.098
14. AES13 (疑似 RSL)	61.33	16.304	0.511	100.41	9.959	0.317	156.23	6.401	0.207
15. AES_RDATA2	311.82	3.207	0.714	498.26	2.007	0.444	733.14	1.364	0.292
16. AES_RDATA1	283.13	3.432	0.701	451.88	2.213	0.435	663.13	1.508	0.289
17. Camellia	69.78	14.330	0.572	112.20	8.913	0.355	169.81	5.889	0.225
18. CAST	33.36	29.889	0.483	54.14	18.471	0.305	81.91	12.209	0.203
19. DES	143.29	6.979	0.510	228.99	4.367	0.320	342.35	2.921	0.211
20. ECC	63.16	15.933	0.435	101.62	9.841	0.268	153.63	6.509	0.163
21. MISTY1	29.46	33.943	0.485	47.68	20.971	0.301	72.58	13.778	0.205
22. RSA	30.60	32.683	0.475	51.32	19.486	0.286	80.22	12.466	0.165
23. SASEBO_ALGO_INPUT	30.51	32.778	0.362	49.83	20.068	0.233	75.67	13.125	0.150
24. SASEBO_ALGO_OUTPUT	340.60	2.936	0.513	541.42	1.847	0.315	817.66	1.223	0.202
25. SASEBO_INPUT	620.35	1.612	0.469	1007.0	0.993	0.273	1477.1	0.677	0.173
26. SASEBO_REG	53.31	18.759	0.197	84.01	11.904	0.197	123.03	8.128	0.121
27. SASEBO_VALUE	-	-	-	-	-	-	-	-	-
28. SEED	29.09	34.38	0.508	47.54	21.033	0.313	73.13	13.674	0.204
29. T_DES	103.80	9.634	0.508	165.92	6.027	0.319	248.20	4.029	0.205

本 LSI では 7 層の金属配線を使用しており, 図 4.4 は電源ラインを除いた信号線を, 各層ごとに示したものである. また図 4.5~4.8 はチップ全体のセルに対する電源供給の様子を示している. まず, チップ外周に 6~7 層配線で VDD/VSS 電源リングが構成され, そこから 4~7 層のメッシュによってチップ全体に電源が供給される. 各セルへの供給は 4 層配線のストライプから Stack Via によって行われる. なお, IO バッファへの VDD/VSS の引き込はそれぞれ, 2 層/3 層配線を使用している.

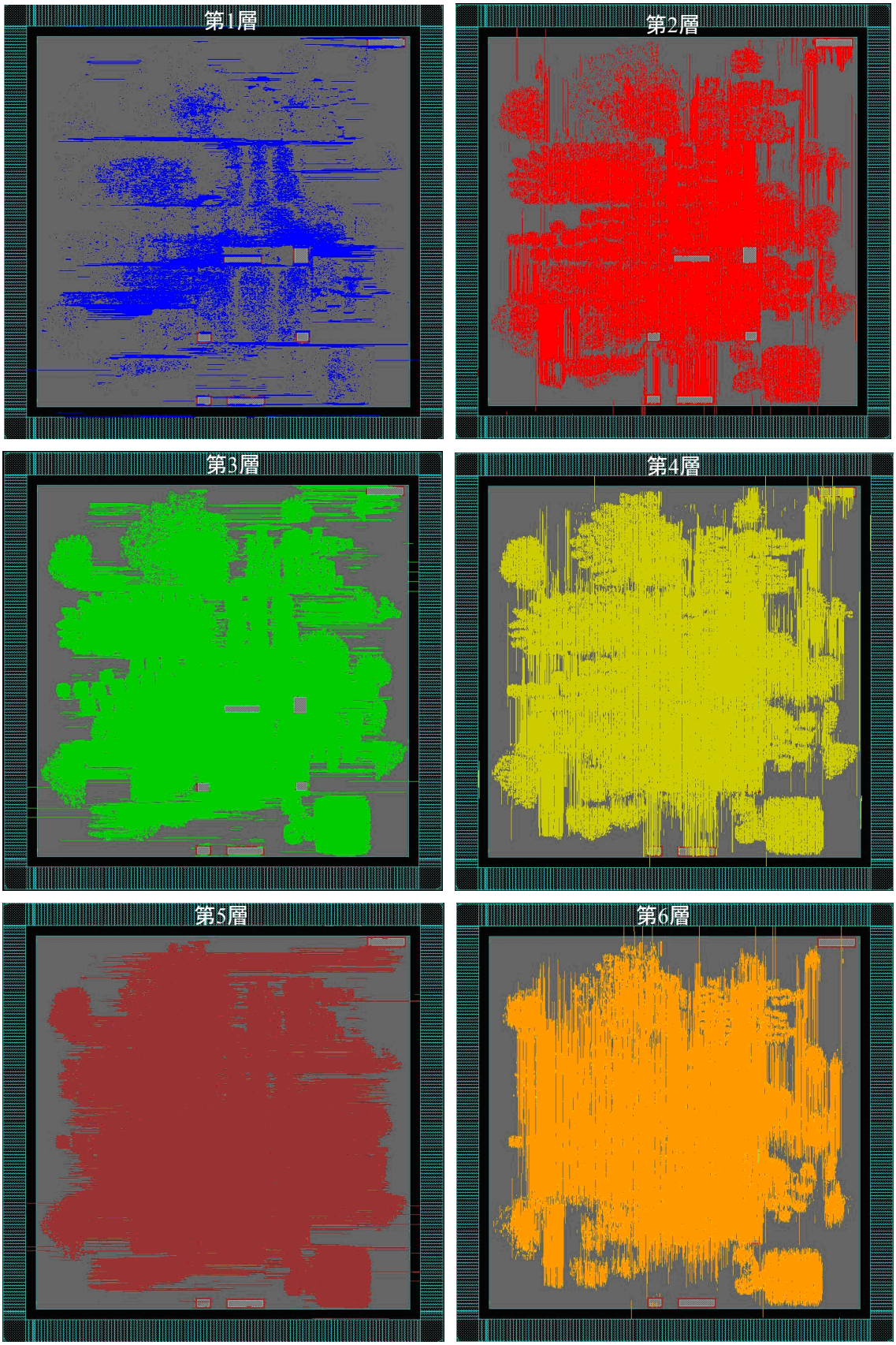


図 4.4　全レイヤの信号線パターン (その 1)

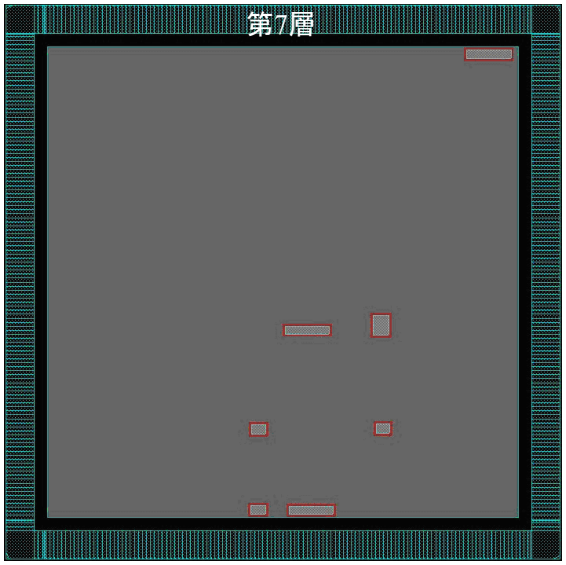


図4.4　全レイヤの信号線パターン (その2)

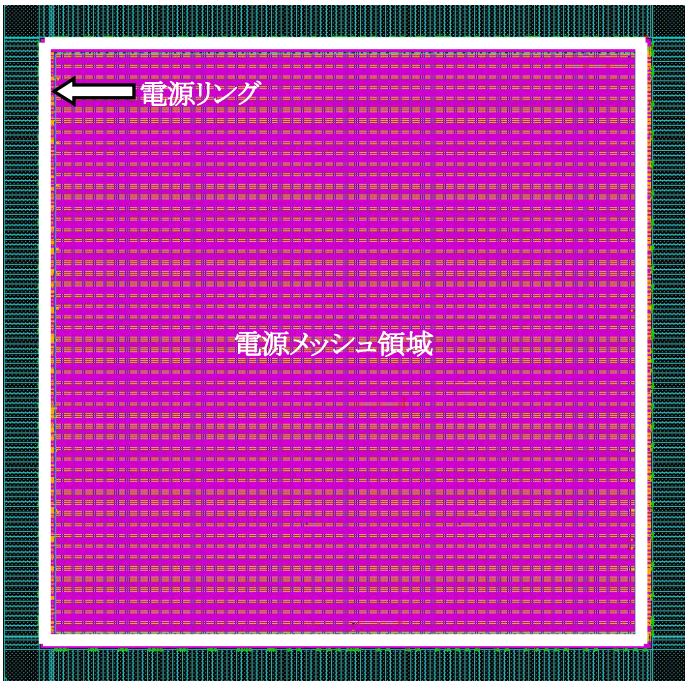


図 4.5　電源配線イメージ

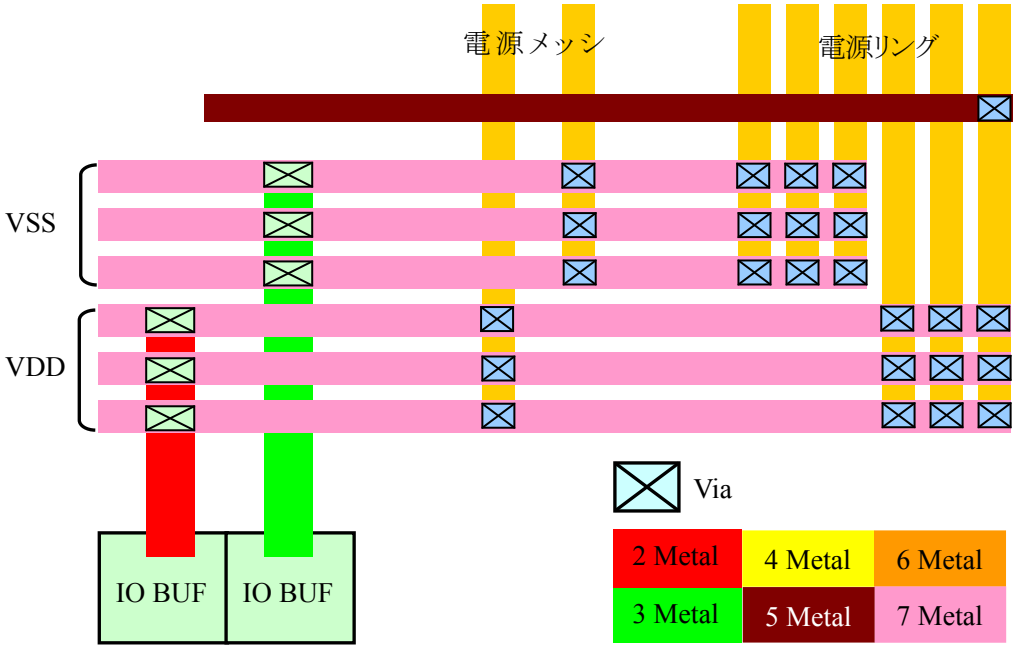


図 4.6 電源リング

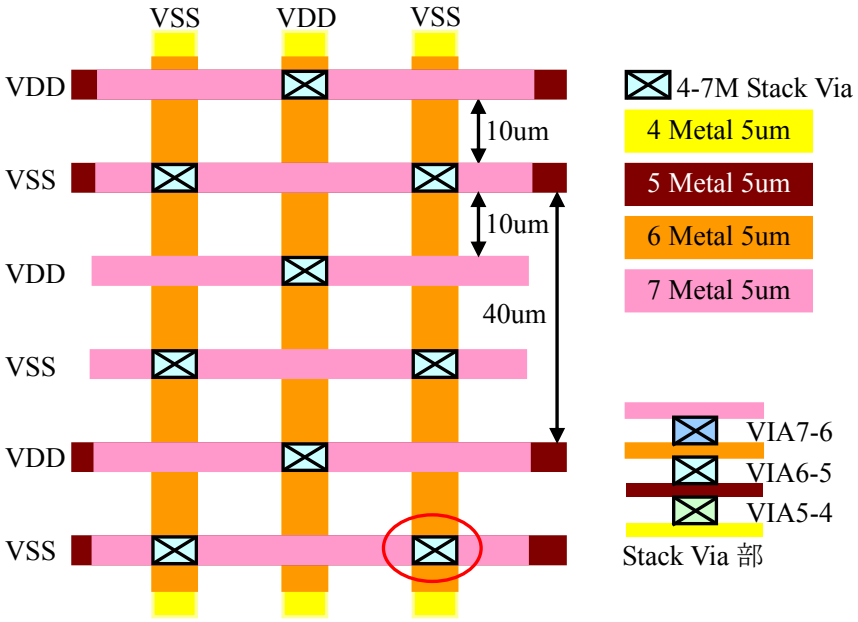


図 4.7 電源メッシュ構造

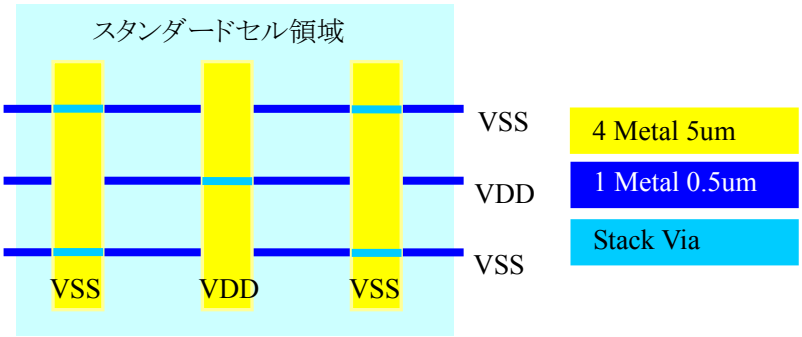


図 4.8 セルへの電源供給

図 4.9 は電源層の配線を抽出したものである. また, 表 4.8 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圧降下で, 図 4.10 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を示している. 電圧降下は 0.4.253 %と極めて小さい上, 実際には 22 個の暗号マクロのうち一度に 1 つしか動作しないので, 通常動作において問題とならない値である.

表 4.8 VDD/VSS 電圧降下

	VDD	VSS
動作周波数	24 MHz	
遷移確率	30 %	
消費電力	109.429 mW	
Worst drop 値	5.104 mV	4.333 mV
Drop 率	0.4253 %	0.3.611 %

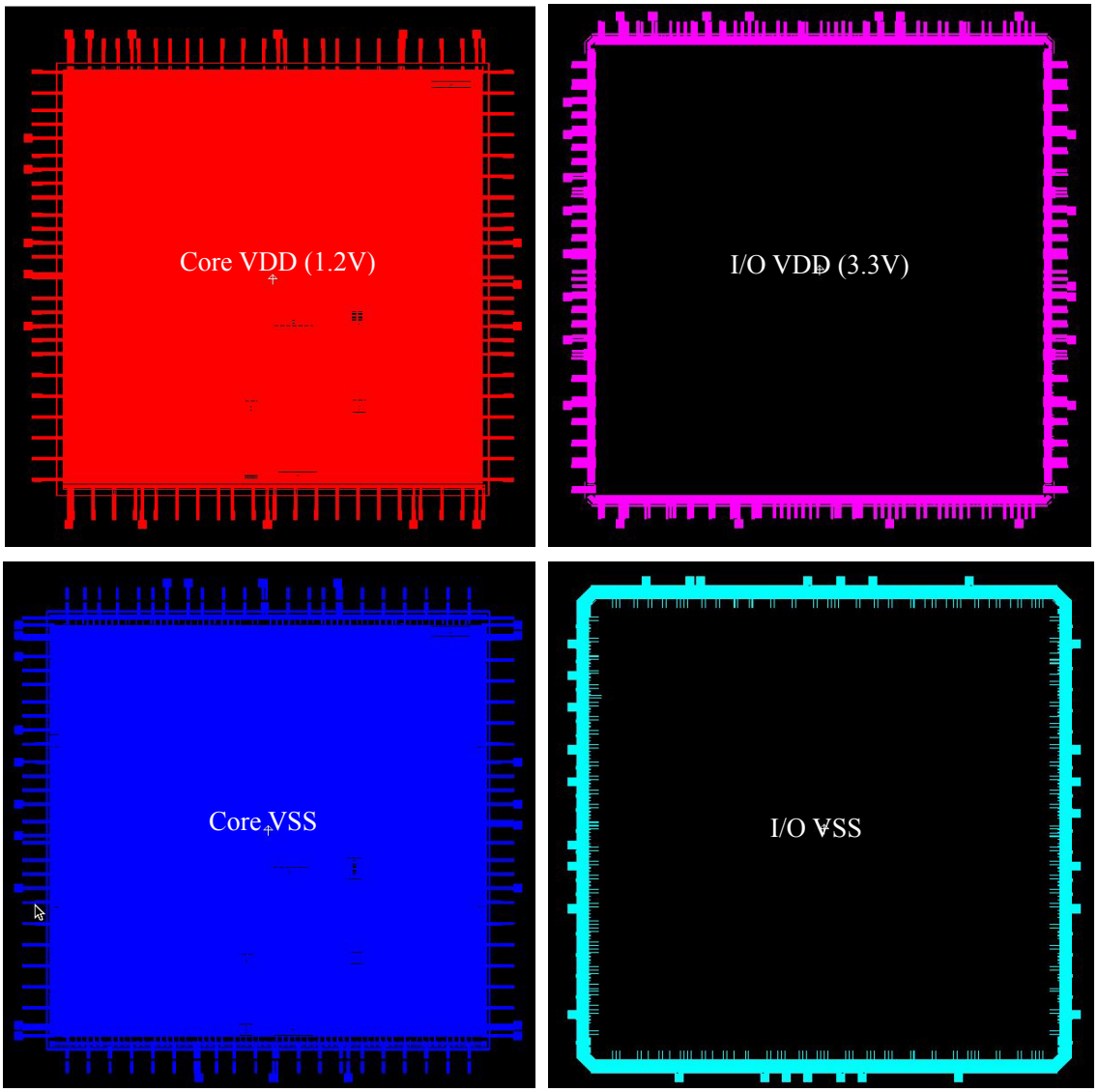
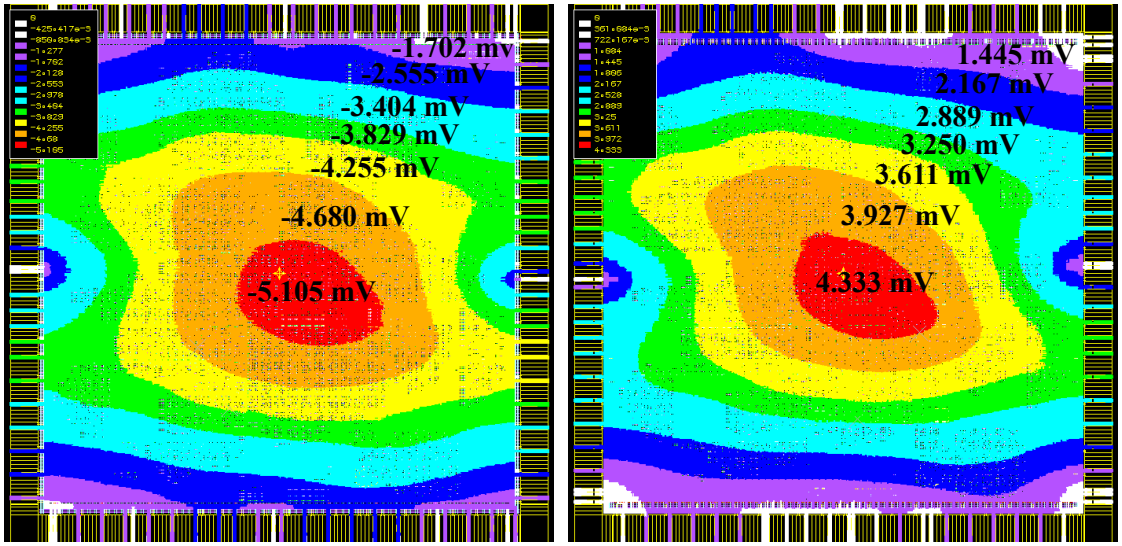


図 4.9 電源ラインの配線パターン



(a) IR-DROP(VDD)　　(b) IR-DROP(VSS)

図 4.10　VDD/VSS の電圧降下

4.2　90nm バージョン

90nm スタンダードセルライブラリを用いた暗号 LSI の論理合成後のレイアウト情報について説明する. 表 4.9 は LSI の概要であり, 4×4 mm^2 のダイサイズのうち, 19.43%のゲートを使用している. 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 4.9　暗号 LSI の概要

項目	
テクノロジ	90nm Logic General Purpose 1P9M 1V-3.3V All Cu Low-k
ウェハプロセス	TSMC CLN90G 90nm CMOS, アルミ 7 層配線
コア電源電圧	1.0±0.10V
I/O 電源電圧	3.3±0.16V
動作周波数	24MHz (41ns)
データエリア	4 × 4 mm^2
セル使用数	2,078,003/10,692,39 (セル面積/セル配置可能面積)
セル使用率	19.43%
PAD 数	160 個
カスタムセル	SRAM

表 4.10　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	Z-2007.03-SP5
配置･配線	SOC Encounter	Cadence	V06.20-s285_1
RC 抽出	Star-RCXT	Synopsys	Z-2006.12-SP1
クロストーク抽出	CeltIC	Cadence	V06.20-s075_1
STA	PrimeTimeSI	Synopsys	Z-2007.06.-SP3
レイアウト検証	Calibre	Mentor	V2008.3-25.16
Power 検証	AstroRail	Synopsys	Z-2007.03-SP8
等価検証	Formality	Synopsys	Z-2007.06.SP-3

表 4.11　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 CLN90G) FB	A0173
	SAGE-X Standard Cells (TSMC CLN90G)　FX – CeltIC	2005q3v2
Digital I/O	In-line, I/O, TPDN90G3, 1.0V/3.3V, (TSMC CLN90G)	130a
RAM	2P-RF ADV (TSMC CLN90G) FB	2008Q3V1
	SP-RF ADV (TSMC CLN90G) FB	2007Q2V1

表 4.12　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	2ns
出力遅延	2ns
外部負荷容量	20pf
仮想配線遅延	tsmc90_w110

図 4.11 は暗号 LSI の電源ラインを除いた Top View を，図 4.12 はレジスタアレイの配置を，図 4.13 は各暗号モジュールの配置を示している．また，表 4.13 はそれらモジュールの回路規模の一覧である．また，表 4.14 はプロセスパラメータとして寄生抵抗と容量を変化させたときの，各動作条件 Worst (125℃ 0.9V), Typical (25℃ 1.0V), Best (-40℃ 1.1V)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 4.15 は暗号モジュール毎の動作速度を示したものである．最も遅いモジュールはサイドチャネル攻撃対策の疑似 RSL2 (Random Switching Logic)を用いた AES 回路で，Worst 条件に置いて動作周波数 20.75 MHz（Typical: 35.56MHz, Best: 38.99MHz）であった．表 4.14 より LSI 全体で最も低速なだったのはプロセスパラメータの寄生容量が Worst で動作条件も Worst の場合で，最大動作周波数 30.468MHz (Typical: 35.319MHz, Best: 38.799MHz) と 24MHz 動作を達成している．

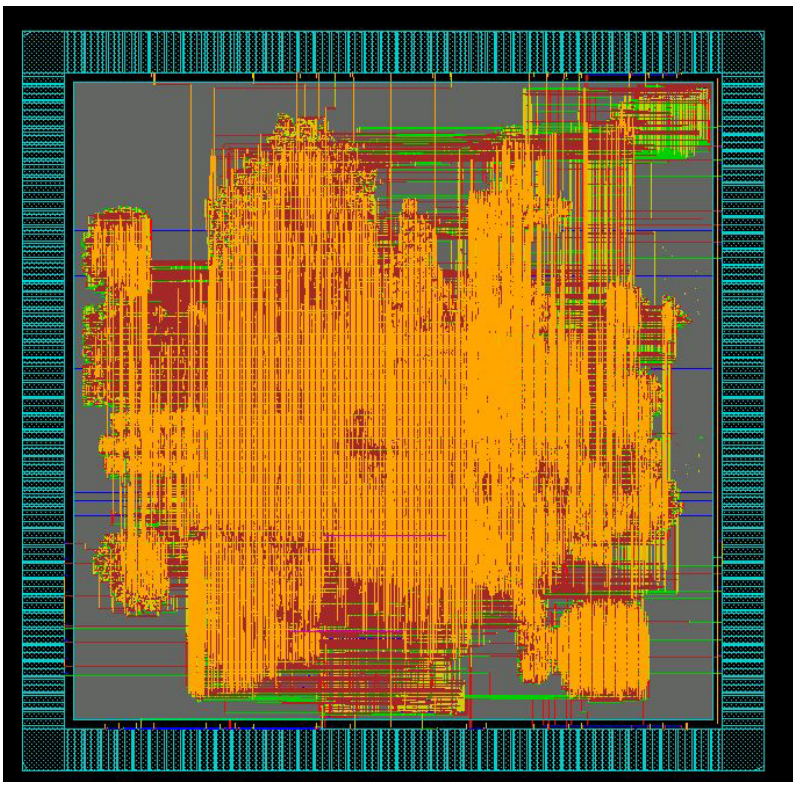


図 4.11　暗号 LSI の Top View

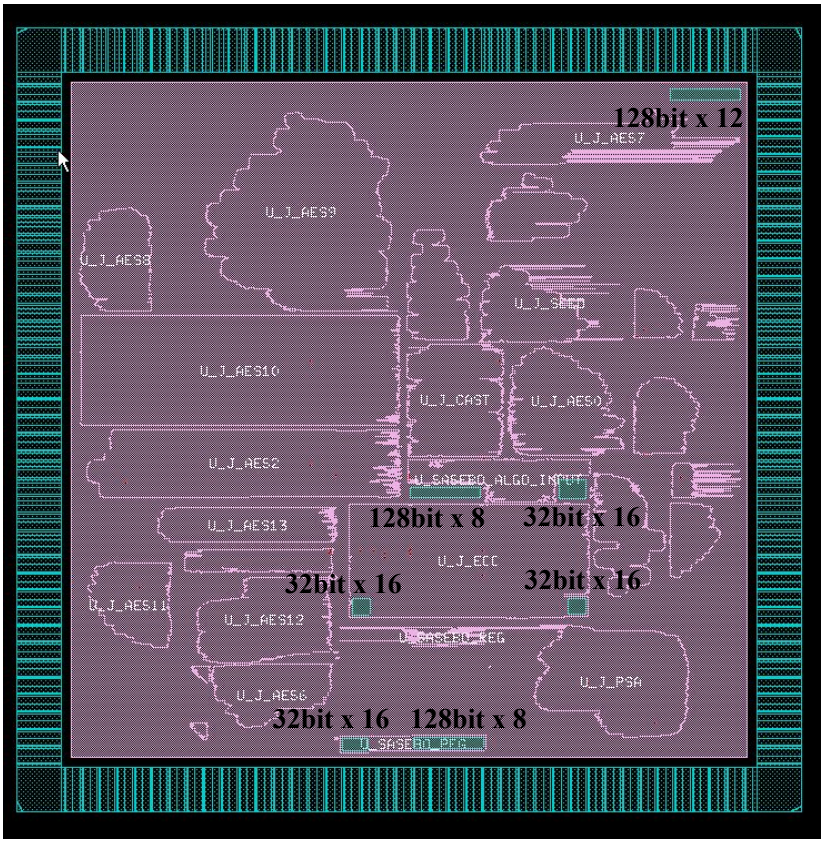


図 4.12　レジスタアレイ配置図

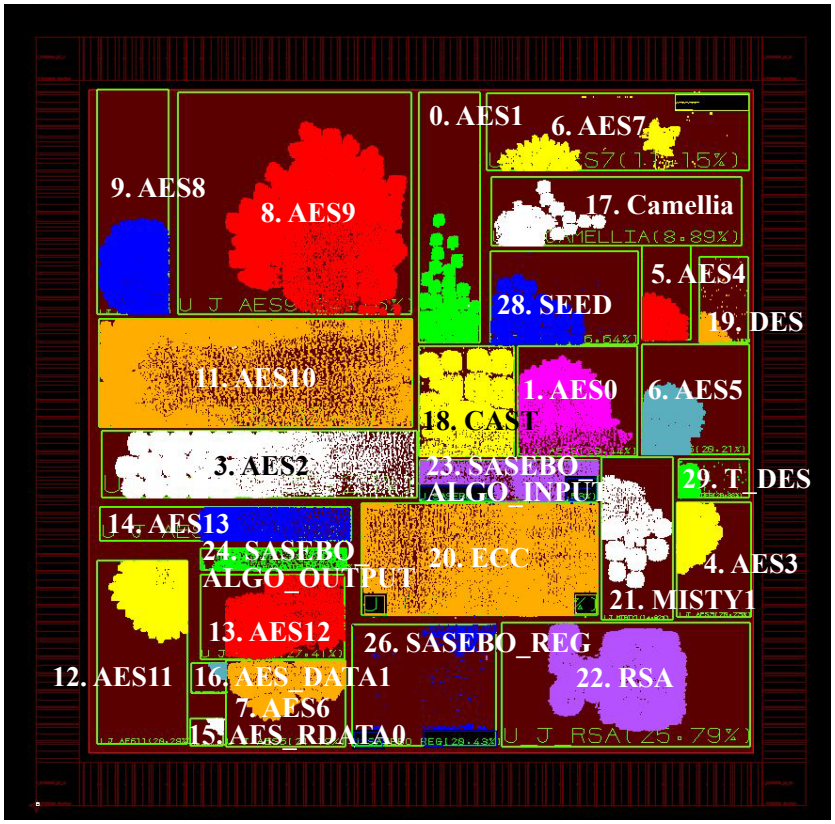


図4.13　暗号モジュール配置図

表 4.13 モジュール面積一覧

モジュール名	面積 (μm^2)	面積 (%)	ゲート数
1. AES0 (合成体 S-box)	64,111	2.5	22,715
2. AES1 (テーブル S-box)	52,958	2.1	18,763
3. AES2 (1-stage PPRM S-box)	152,991	5.9	54,206
4. AES3 (3-stage PPRM S-box)	41,358	1.6	14,653
5. AES4 (合成体 S-box)	29,921	2.0	10,601
6. AES5 (CTR モード)	58,430	2.2	20,702
7. AES6 (FA 対策済)	50,721	2.0	17,971
8. AES7 (ラウンド鍵事前生成)	54,855	2.1	19,436
9. AES8 (MAO)	87,345	3.3	30,947
10. AES9 (MDPL)	306,231	11.6	108,500
11. AES10 (Threshold)	269,448	10.5	95,468
12. AES11 (WDDL)	83,206	3.2	29,480
13. AES12 (疑似 RSL)	80,511	3.1	28,526
14. AES13 (疑似 RSL)	46,131	1.8	16,344
15. AES_RDATA2	3,014	0.1	1,068
16. AES_RDATA1	3,018	0.1	1,069
17. Camellia	35,633	1.4	12,625
18. CAST	71,445	2.8	25,313
19. DES	8,058	0.3	2,855
20. ECC	168,459	6.6	59,686
21. MISTY1	41,051	1.6	14,545
22. RSA	191,661	7.4	67,907
23. SASEBO_ALGO_INPUT	22,195	1.1	7,864
24. SASEBO_ALGO_OUTPUT	13,572	0.6	4,809
25. SASEBO_INPUT	1,082	0.0	383
26. SASEBO_REG	86,867	3.3	30,778
27. SASEBO_VALUE	315	0.0	112
28. SEED	55,425	2.1	19,638
29. T_DES	13,377	0.5	4,740
Total cell area	2,557,262	100.00	906,059

1 ゲート = 2 入力 NAND (2.52μm × 1.12μm)

表 4.14 Static Timing Analysis による LSI の動作速度

プロセス条件	項目	Worst (125℃ 0.9V)	Typical (25℃ 1.0V)	Best (-40℃ 1.1V)
寄生容量 Best	Maximum Frequency	30.902 MHz	35.690 MHz	39.095 MHz
	Critical Path	32.360 ns	28.019 ns	25.579 ns
	Hold Time	0.117 ns	0.066 ns	0.037 ns
寄生抵抗・容量 Best	Maximum Frequency	30.469 MHz	35.314 MHz	38.790 MHz
	Critical Path	32.820 ns	28.317ns	25.780 ns
	Hold Time	0.122 ns	0.077 ns	0.042 ns
寄生抵抗・容量 Typical	Maximum Frequency	30.747 MHz	35.556 MHz	38.989 MHz
	Critical Path	32.524 ns	28.125 ns	25.648 ns
	Hold Time	0.122 ns	0.079 ns	0.043 ns
寄生容量 Worst	Maximum Frequency	30.468 MHz	35.319 MHz	38.799 MHz
	Critical Path	32.821 ns	28.313 ns	25.734 ns
	Hold Time	0.137 ns	0.087 ns	0.048 ns
寄生抵抗・容量 Worst	Maximum Frequency	30.917 MHz	35.696 MHz	39.093 MHz
	Critical Path	32.344 ns	28.014 ns	25.580 ns
	Hold Time	0.136 ns	0.078 ns	0.046 ns

表 4.15 Static Timing Analysis による各暗号モジュールの動作速度 (Typical プロセス時)

ブロック名	Worst (125℃ 0.9V)			Typical (25℃ 1.0V)			Best (-40℃ 1.1V)		
	Freq. (MHz)	Critic. (ns)	Hold (ns)	Freq (MHz)	Critic. (ns)	Hold (ns)	Freq (MHz)	Critic. (ns)	Hold (ns)
1. AES0 (合成体 S-box)	144.30	8.749	0.288	181.42	5.512	0.164	312.30	3.202	0.104
2. AES1 (テーブル S-box)	153.44	6.517	0.276	249.56	4.007	0.165	402.41	2.485	0.107
3. AES2 (1-stage PPRM S-box)	55.50	18.017	0.275	88.30	11.325	0.159	165.07	6.058	0.104
4. AES3 (3-stage PPRM S-box)	157.13	6.364	0.279	257.20	3.888	0.159	434.22	2.303	0.104
5. AES4 (合成体 S-box)	154.99	6.452	0.287	250.31	3.995	0.169	426.62	2.344	0.105
6. AES5 (CTR モード)	59.69	16.753	0.237	99.28	10.073	0.139	152.51	6.557	0.088
7. AES6 (FA 対策済)	81.73	12.236	0.267	131.56	7.601	0.148	210.13	4.759	0.094
8. AES7 (ラウンド鍵事前生成)	150.24	6.656	0.261	242.31	4.127	0.154	418.76	2.388	0.093
9. AES8 (MAO)	98.75	10.127	0.200	160.49	6.231	0.118	290.44	3.443	0.070
10. AES9 (MDPL)	40.88	24.461	0.199	71.27	14.032	0.119	114.26	8.752	0.075
11. AES10 (Threshold)	81.89	12.211	0.225	129.30	7.734	0.141	226.55	4.414	0.084
12. AES11 (WDDL)	92.40	10.823	0.192	155.62	6.426	0.119	262.05	3.816	0.077
13. AES12 (疑似 RSL)	30.75	32.524	0.200	35.56	28.125	0.120	38.99	25.648	0.066
14. AES13 (疑似 RSL)	92.34	10.829	0.216	147.84	6.764	0.127	251.07	3.983	0.066
15. AES_RDATA2	568.18	1.760	0.345	929.37	1.076	0.212	1420.5	0.704	0.129
16. AES_RDATA1	583.43	1.714	0.327	956.94	1.045	0.198	1483.7	0.674	0.125
17. Camellia	106.55	9.385	0.291	171.12	5.844	0.181	272.41	3.671	0.108
18. CAST	48.82	20.484	0.251	80.46	12.428	0.144	130.26	7.677	0.092
19. DES	256.67	3.896	0.298	419.11	2.386	0.183	681.66	1.467	0.099
20. ECC	107.70	9.285	0.150	170.77	5.856	0.089	277.24	3.607	0.054
21. MISTY1	42.05	23.784	0.292	68.58	14.581	0.166	108.61	9.207	0.111
22. RSA	62.02	16.123	0.241	104.54	9.566	0.136	167.84	5.958	0.086
23. SASEBO_ALGO_INPUT	50.36	19.856	0.317	83.34	11.999	0.181	127.89	7.819	0.115
24. SASEBO_ALGO_OUTPUT	659.63	1.516	0.284	1061.6	0.942	0.175	1655.6	0.604	0.107
25. SASEBO_INPUT	1485.9	0.673	0.211	2433.1	0.411	0.124	3703.7	0.270	0.075
26. SASEBO_REG	98.58	10.144	0.204	155.09	6.448	0.121	233.15	4.289	0.074
27. SASEBO_VALUE	-	-	-	-	-	-	-	-	-
28. SEED	36.33	27.529	0.255	60.85	16.435	0.150	97.59	10.247	0.096
29. T_DES	199.40	5.015	0.292	328.95	3.050	0.175	546.15	1.831	0.102

本 LSI は 7 層の金属配線を使用しており，図 4.14 は電源ラインを除いた信号線を，各層ごとに示したものである．チップ全体のセルに対する電源供給プランは 130nm 版の図 4.6~4.8 と，まったく同一であり，配線幅・スペースも同じ値を採用している．

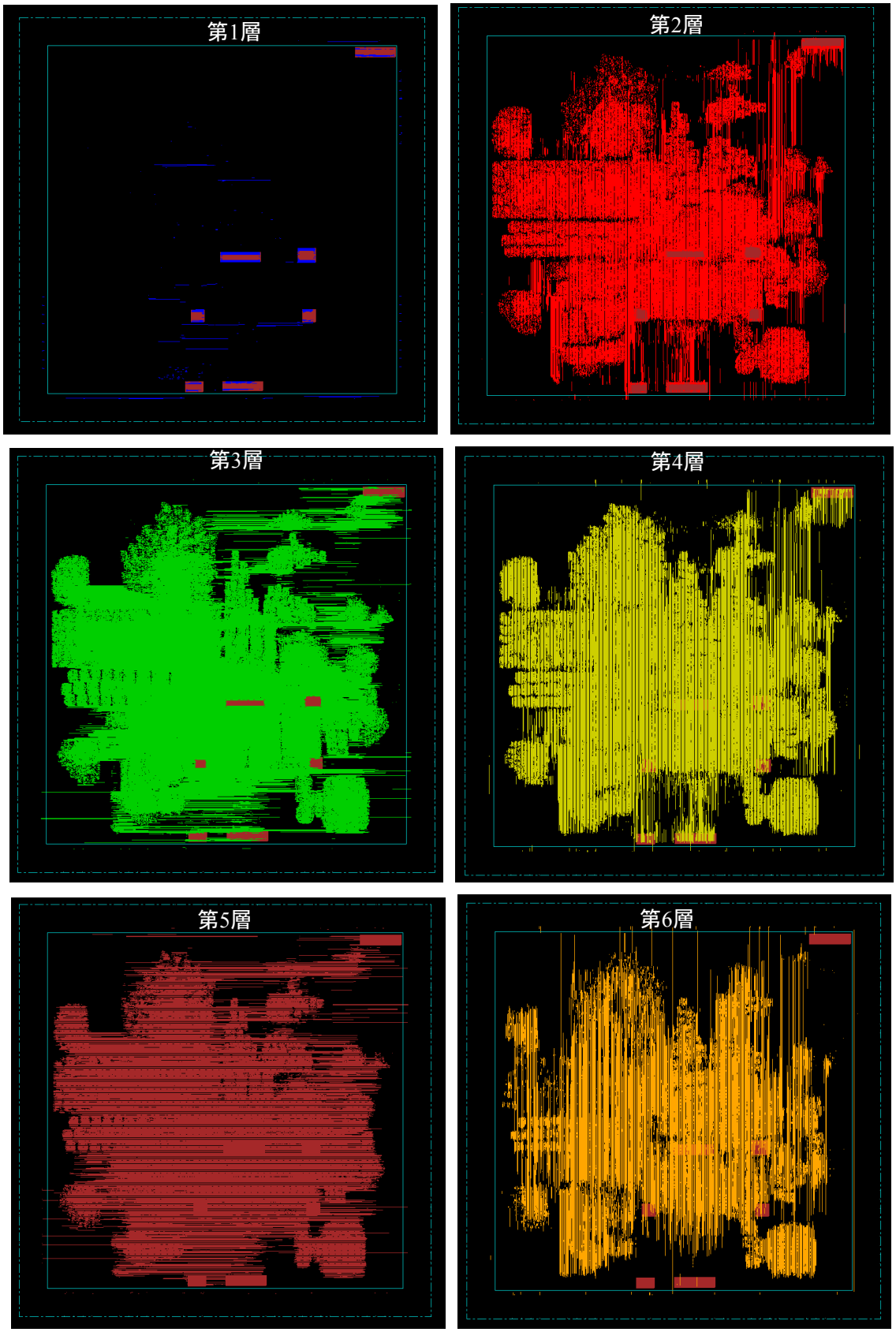


図 4.14　全レイヤの信号線パターン (その 1)

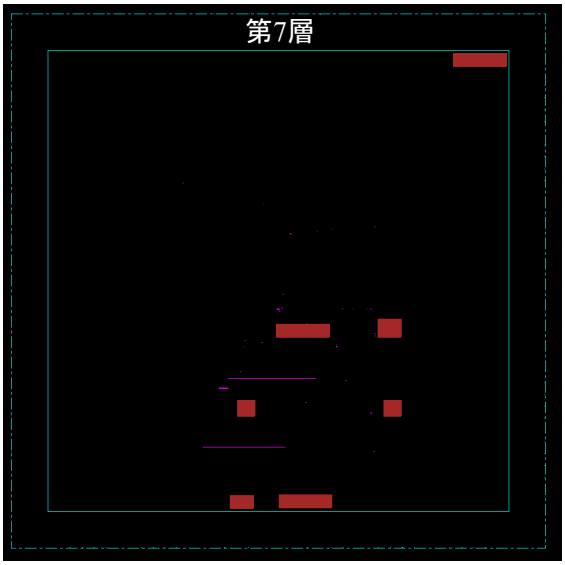


図4.14　全レイヤの信号線パターン (その2)

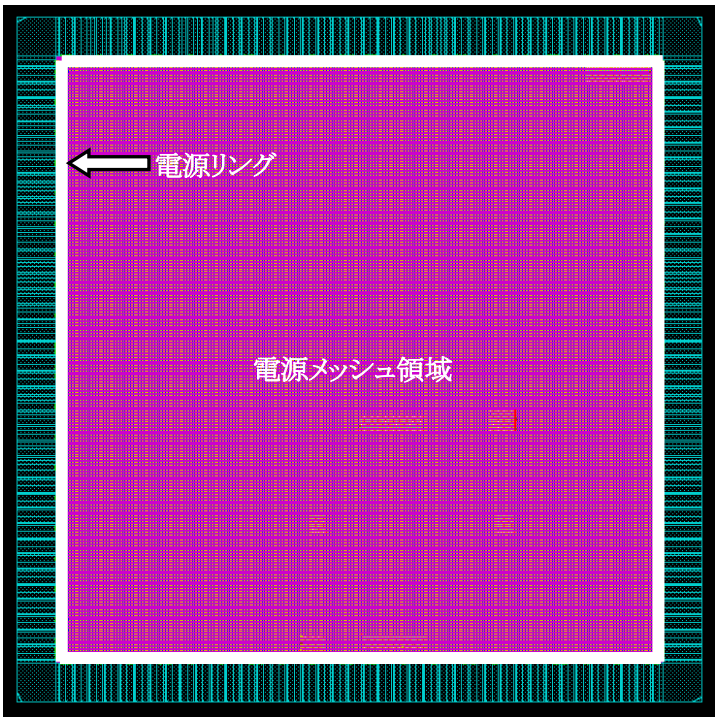


図 4.15　電源配線イメージ

図 4.16 は電源層の配線を抽出したものである．また，表 4.16 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圧降下で，図 4.17 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を示している．電圧降下は 0.3224%と極めて小さい上，実際には 22 個の暗号マクロのうち一度に 1 つしか動作しないので，通常動作時においては問題とならない値である．

表 4.16　VDD/VSS 電圧降下

	VDD	VSS
動作周波数	24 MHz	
遷移確率	30 %	
消費電力	49.9154 mW	
Worst drop 値	2.763 mV	3.224 mV
Drop 率	0.2763 %	0.3224 %

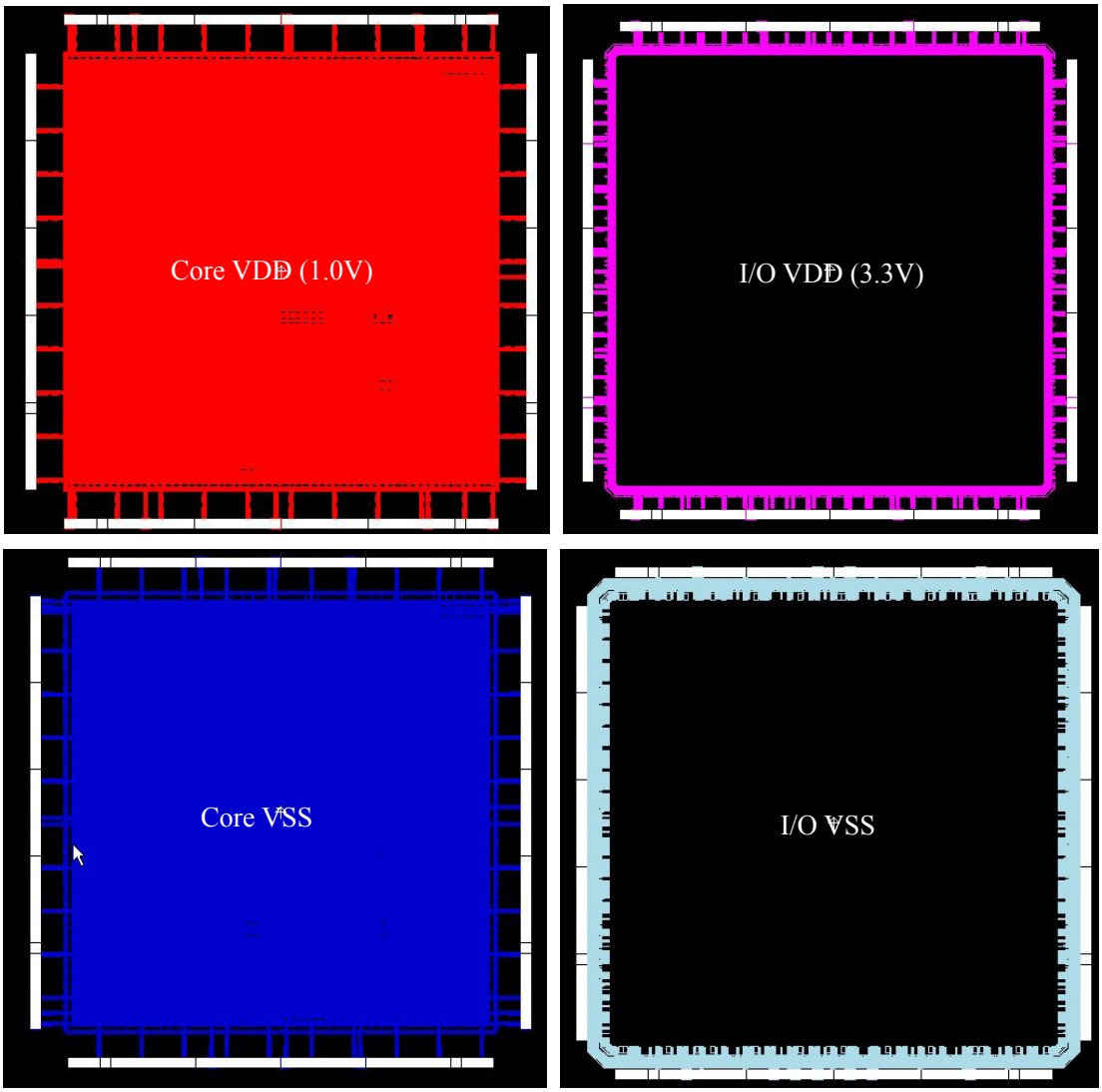
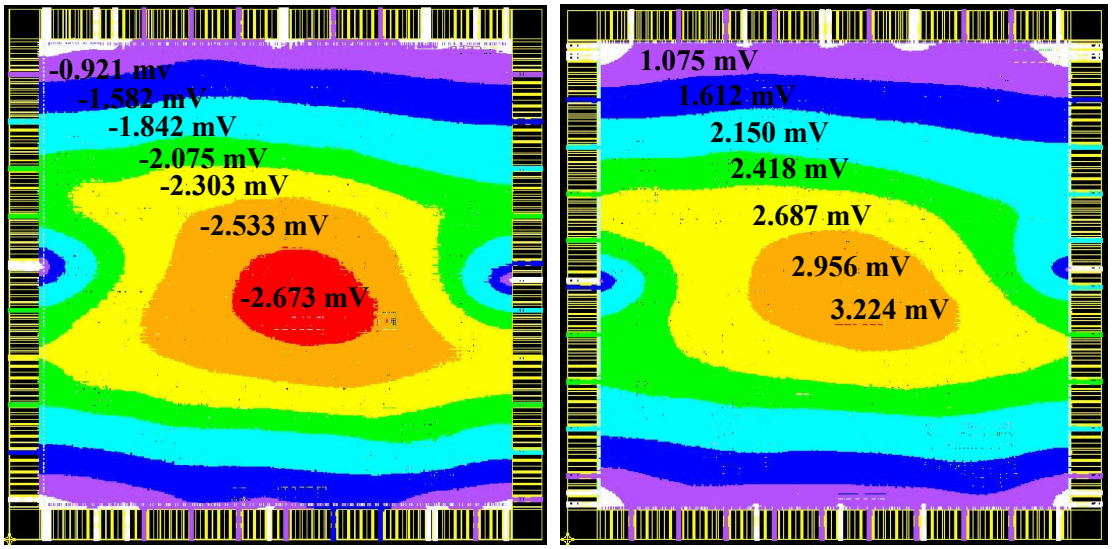


図 4.16　電源ラインの配線パターン



(a) IR-DROP(VDD)　　(b) IR-DROP(VSS)

図 4.17　VDD/VSS の電圧降下

5. 暗号ハードウェア IP コア

5.1 AES0 (合成体 S-box)

AES 暗号マクロ AES0 の概要を表 5.1 に, I/O ポートを表 5.2 に示す. アルゴリズムの詳細は“FIPS PUB 197: ADVANCED ENCRYPTION STANDARD (AES)”[2)]を参照されたい. 暗号 LSI ではユーザが設定できる鍵長が 56bit に制限されているが, 本マクロ自体は 128bit の鍵による暗号化と復号をサポートしている.

表 5.1 AES0 の概要

アルゴリズム	AES
データブロック長	128 bits
鍵長	128 bits
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	AES_Comp.v
記述言語	Verilog-HDL
トップモジュール名	AES_Comp_ENC_top
S-box	合成体 GF(((2^2)^2)^2)ベース
スループット	128 bit / 10 clock
ラウンド鍵生成	On-the-fly

表 5..2 AES0 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に ‘1’ が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 128bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 AES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.

Kvld	Out	1	鍵初期化処理が完了すると，1 クロックの間だけ Kvld=1 となり，次のクロックですぐに 0 の落とされる．この後すぐに暗号化および復号処理が実行可能となる．
Dvld	Out	1	暗号化(または復号)処理が完了し，暗号文(または平文)がデータ出力ポート Dout にセットされると，1 クロックの間だけ Dryd=1 となり，次のクロックですぐに 0 に落とされる．

AES0 は図 5.1 に示した暗号化回路と図 5.2 の復号回路の 2 つの回路ブロックから構成され，両者でレジスタやデータパスの共有化は行っていない．S-box は合成体 $GF(((2^2)^2)^2)$上で定義された乗法逆元回路 [3]を使用している．

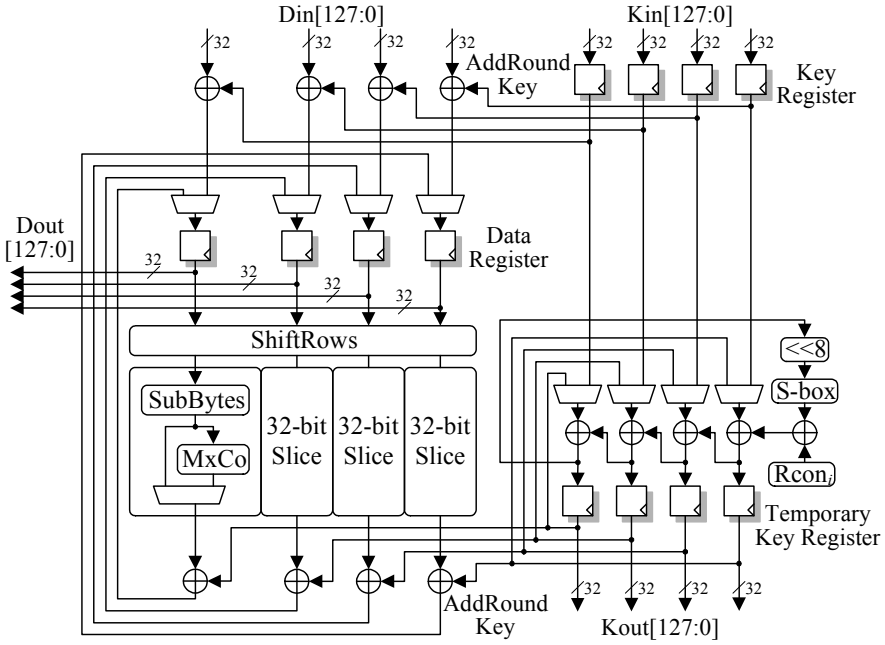


図 5.1　AES0 の暗号化処理のデータパス

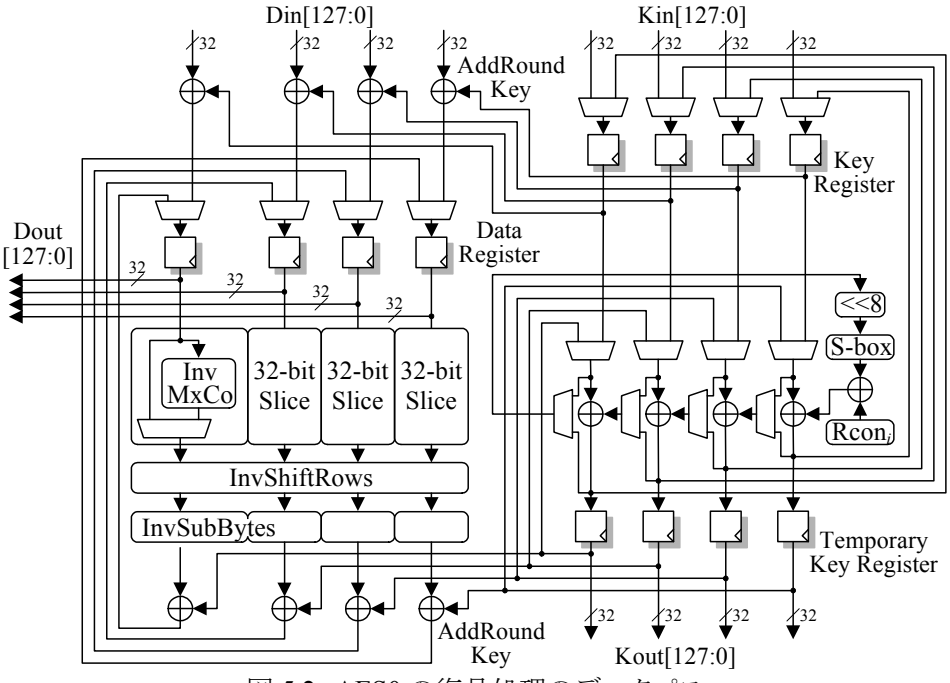


図 5.2　AES0 の復号処理のデータパス

図 5.3 に最短サイクルでの暗号化処理のタイミングチャートを示す．各クロックの動作は下記の通りである．

CLK1: RSTn=0 とすることで，制御回路がリセットされる．
CLK2: Krdy=1 とすることで，Kin に入力された 128bit の秘密鍵が内部レジスタにセットされる．
CLK3: EncDec=0 なので暗号化処理であるが，復号処理ブロック側で復号処理の最初のラウンド鍵（暗号化処理の最終ラウンド鍵）を生成する初期化が開始され，ビジー信号 BSY=1 となる．Kout には暗号化処理側の回路ブロックからの出力が接続されているので，鍵初期化時にラウンド鍵は出力されない．
CLK14: 鍵の初期化が終了し，BSY=0，また 1 クロックだけ Kvld=1 となる．それと同時に Din に入力された 128bit の平文が内部レジスタにセットされる．
CLK15: EncDec＝0 なので暗号化処理が開始され，ビジー信号 BSY=1 となる．これから毎クロック，Kout に Temporary Key Register のラウンド鍵が出力されていく．
CLK16~25: 暗号化処理は 10 クロックを要し，CLK24 で完了する．128bit の暗号文が Dout から出力され，BSY=0，データ出力信号 Dvld が 1 クロックだけ 1 となる．

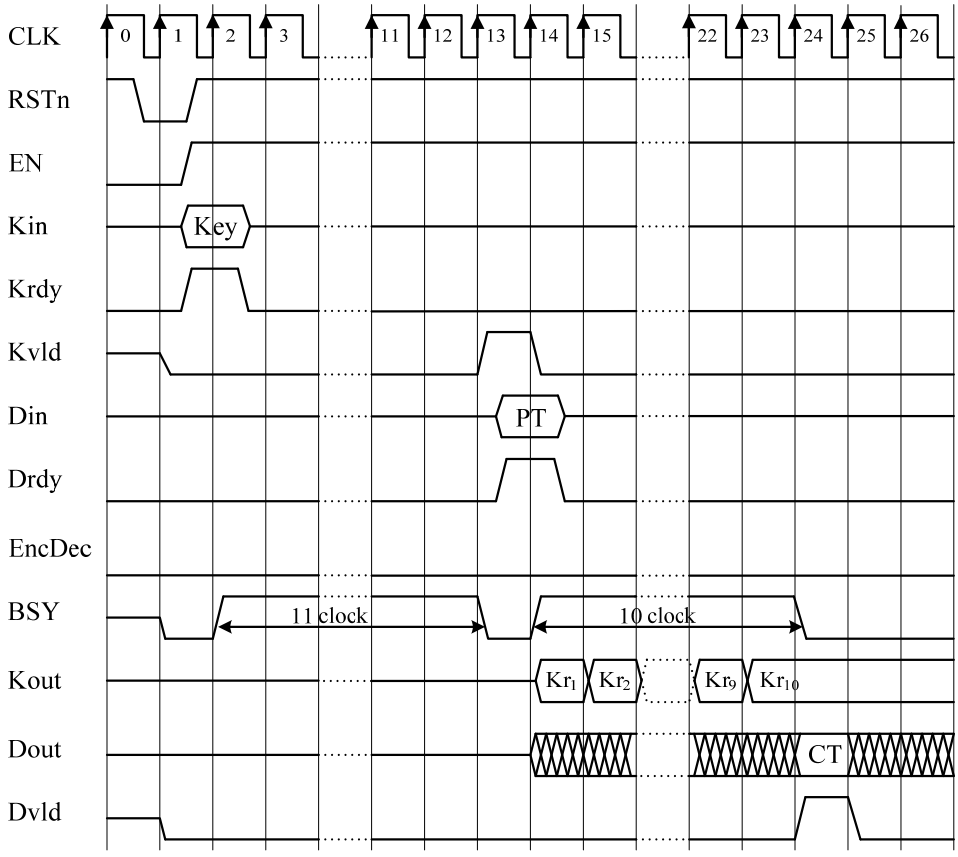


図 5.3　AES0 の暗号化処理のタイミングチャート

図 5.4 に最短サイクルでの復号処理のタイミングチャートを示す．各クロックの動作は下記の通りである．

CLK1: RSTn=0 とすることで，制御回路がリセットされる．
CLK2: Krdy=1 とすることで，Kin に入力された 128bit の秘密鍵が内部レジスタにセットされる．
CLK3:復号処理の最初のラウンド鍵（暗号化処理の最終ラウンド鍵）を生成する初期化が開始され，ビジー信号 BSY=1 となる．
CLK14: 鍵の初期化が終了し，BSY=0，また 1 クロックだけ Kvld=1 となる．それと同時に Din に入力された 128bit の暗号文が内部レジスタにセットされる．

CLK15: EncDec＝1 なので復号処理が開始され，ビジー信号 BSY=1 となる．これから毎クロック，Kout に Temporary Key Register のラウンド鍵が出力されていく．

CLK16~25: 復号処理は暗号化処理と同様に 10 クロックを要し，CLK25 で完了する．128bit の平文が Dout から出力され，BSY=0，データ出力信号 Dvld が 1 クロックだけ 1 となる．

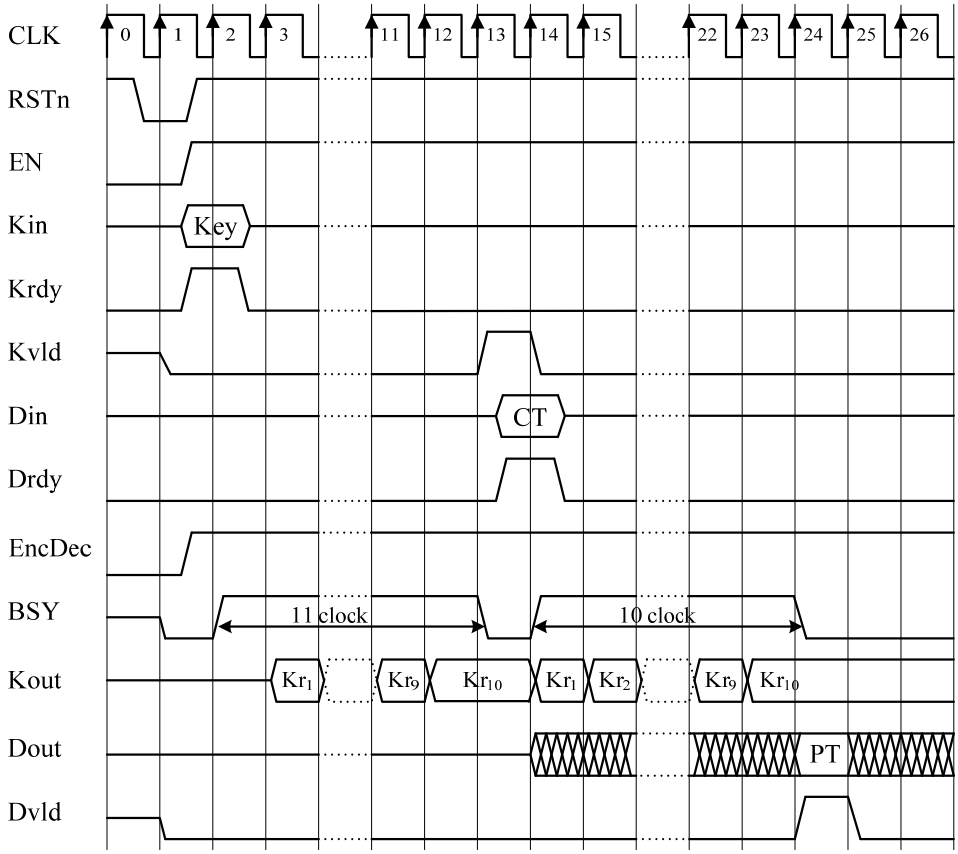


図 5.4　AES0 の復号処理のタイミングチャート

5.2　AES1/AES2/AES3/AES4（各種 S-box 実装）

AES 暗号回路マクロ AES1/AES2/AES3/AES4 は，S-box の違いによるサイドチャネル攻撃耐性の差を比較評価するためのものであり，S-box の構造だけが異なっている．AES1 はルックアップテーブル実装を，AES2/3 は PPRM(Positive Polarity Reed-Muler)ロジック[4]による実装を，AES4 は合成体による乗法逆元回路[3]を用いている．また，暗号化処理だけをサポートし，復号の機能は持たない．従って，AES0 で暗号化と復号を切り替える信号 EncDec を削除したインタフェースとなっている．これらマクロの概要を表 5.3 に，I/O ポートを表 5.4 に示す．データパスアーキテクチャは図 5.1 の AES0 の暗号化回路と同一であるが，秘密鍵を入力したときに行われる(復号回路での)初期化処理が不要なため，図 5.5 で示すタイミングチャートが異なっている．

表 5.3　AES1/AES2/AES/AES4 の概要

アルゴリズム	AES
データブロック長	128 bits
鍵長	128 bits
機能	暗号化
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	AES1: AES_TBL.v

	AES2: ASE_PPRM1.v AES3: AES_PPRM3.v AES4: AES_Comp.v
記述言語	Verilog-HDL
トップモジュール名	AES1: AES_TBL AES2: ASE_PPRM1 AES3: AES_PPRM3 AES4: AES_Comp
S-box	AES1: Look-up Table AES2: PPRM1 AES3: PPRM3 AES4: 合成体 GF(((2^2)^2)^2)
スループット	128 bit / 10 clock
ラウンド鍵生成	On-the-fly

表 5.4 AES1/AES2/AES/AES4 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 128it の平文データが 内部レジスタにラッチされ, 暗号化処理が開始される.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 AES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化あるいは鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化処理が実行可能となる.
Dvld	Out	1	暗号化処理が完了し, 暗号文がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

図 5.5 に最短サイクルでの暗号化処理のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで，制御回路がリセットされる．
CLK2: Krdy=1 により，Kin に入力された 128bit の秘密鍵が内部レジスタにセットされる．
CLK3: 鍵の初期化が終了し，BSY=0，また 1 クロックだけ Kvld=1 となる．それと同時に Din に入力された 128bit の平文が内部レジスタにセットされる．
CLK4: 暗号化処理が開始され，ビジー信号 BSY=1 となる．これから毎クロック，Kout に Temporary Key Register のラウンド鍵が出力されていく．
CLK5~14: 暗号化処理は 10 クロックを要し，CLK14 で完了する．128bit の暗号文が Dout から出力され，BSY=0，データ出力信号 Dvld が 1 クロックだけ 1 となる．

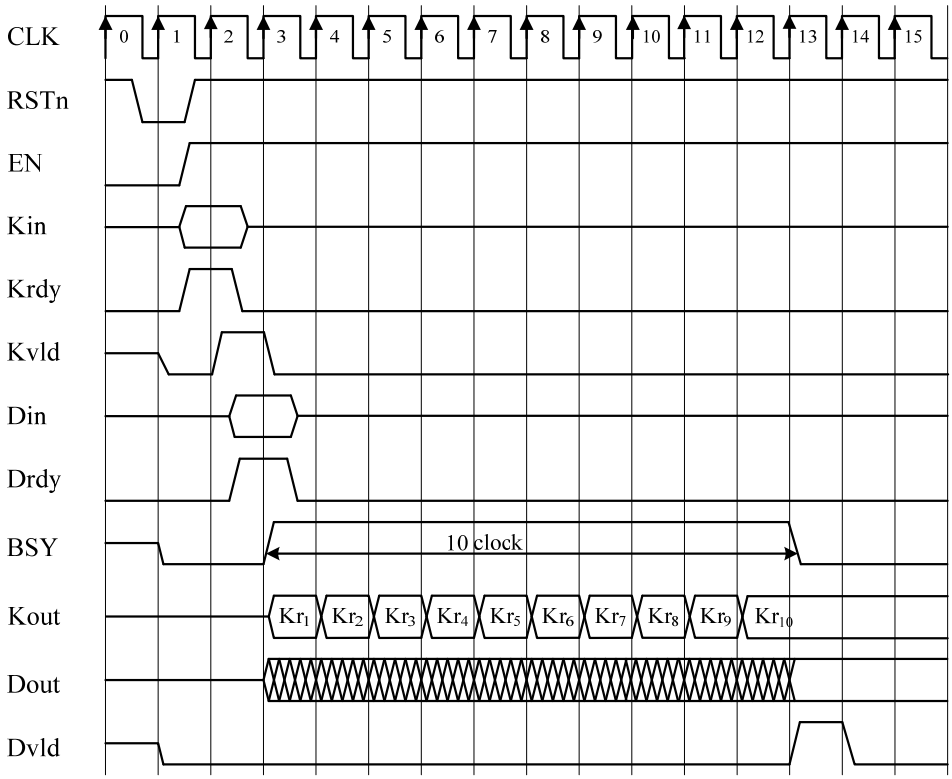


図 5.5 AES1/AES2/AES3/AES4 のタイミングチャート

5.3 AES5 (CTR モード)

AES 暗号回路マクロ AES5 は，CTR モード[5)]をサポートし，4 段のパイプライン処理により高速化を図っている．本マクロの概要を表 5.5 に，I/O ポートを表 5.6 に示す．暗号化と復号はいずれも AES コアが生成する同じ乱数との XOR 処理であり，平文／暗号文の入力が異なるだけで同じ動作となっている．したがって AES0 のように暗号化と復号を切り替える信号 EncDec は有していない．

表 5.5 AES5 の概要

アルゴリズム	AES
データブロック長	128 bits
鍵長	128 bits
機能	暗号化/復号
暗号利用モード	Counter (CTR)
ソースファイル名	AES_CTR_Pipe_Comp.v
記述言語	Verilog-HDL

トップモジュール名	AES
S-box	合成体 GF(((2²)²)²)
スループット	128 bits * 4 blocks / 46 clocks
ラウンド鍵生成	On-the-fly

表 5.6 AES5 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	Drdy=1 かつ Drcv=1 のとき, Din に入力された 128bit の平文(または暗号文)データブロックが, 暗号化(または復号)処理のため内部レジスタにラッチされる. BSY=1 のときでも Drcv=1 であれば, データブロックを連続して入力することができる.
CTRrdy	In	1	BSY=0 の間に CTRrdy=1 とすることで, 暗号処理開始信号 START の状態とは関係なく, 直ちに乱数生成処理が開始される. そして START=1 によって平文(または暗号文)が入力されたときに, 直ちに暗号文(または平文)が出力できるように XOR する乱数が準備される.
START	In	1	連続する 4 ブロックの平文(または暗号文)データが入力され, この信号に START=1 がセットされると, 4 つの乱数が次々と XOR されて暗号文(または平文)が出力される. そして, 次のデータブロックが入力されたときに出力が止まらないように, 次の乱数生成が開始可能となる. スループットを最大とするためには START=1 に保持しておくことが推奨される.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 AES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)が

			データ出力ポート Dout にセットされると，1 クロックの間だけ Dryd=1 となり，次のクロックですぐに 0 に落とされる.
Drcv	Out	1	データ入力許可信号. Drcv=1 のときに限り,暗号文または平文データブロックを入力することができる.

パイプライン処理による CTR モードをサポートした AES 回路のデータパスを図 5.6 に示す. S-box は合成体 $GF(((2^2)^2)^2)$の乗法逆元回路を用いており，その S-box 内部でパイプライン化されている. 左側のランダム化部と右側の鍵スケジュール部は共に 4 段のパイプラインステージを持つ. AES の暗号化部は疑似乱数生成器として用いられ，入力された平文(または暗号文)はその疑似乱数と XOR されて暗号化(または復号化)される. したがって，暗号化と復号では同じ疑似乱数を XOR することになる. 乱数生成用の秘密鍵とカウンタの初期値をそれぞれ 128bit の鍵レジスタ Kreg とカウンタレジスタ CTRreg にセットすると，自動的にカウンタ値がインクリメントされて 4 つのカウンタ値(初期値 +0/+1/+2/+3)が乱数に変換される. 変換中でも，4 ブロックの平文(または暗号文)データが入力可能で，それらは 128bit の 4 つのデータ入力レジスタ RegDI0~RegDI3 にストアされる. カウンタ値の乱数変換後に 4 ブロックのデータを入力することもできるが，その場合は最大のスループットである， 128 * 4 bits / 46 clocks を得ることはできない. データ入力レジスタの平文(または暗号文)は生成された乱数と XOR されながら暗号文(または平文)として出力される. 4 ブロックのデータの暗号化(または復号)が完了すると，カウンタの値は自動的に4回インクリメントされ，新たな乱数生成処理が開始される. 最大のスループットを得るためには，4 ブロックの平文(または暗号文)を，平均して 46 クロック毎に入力する必要がある.

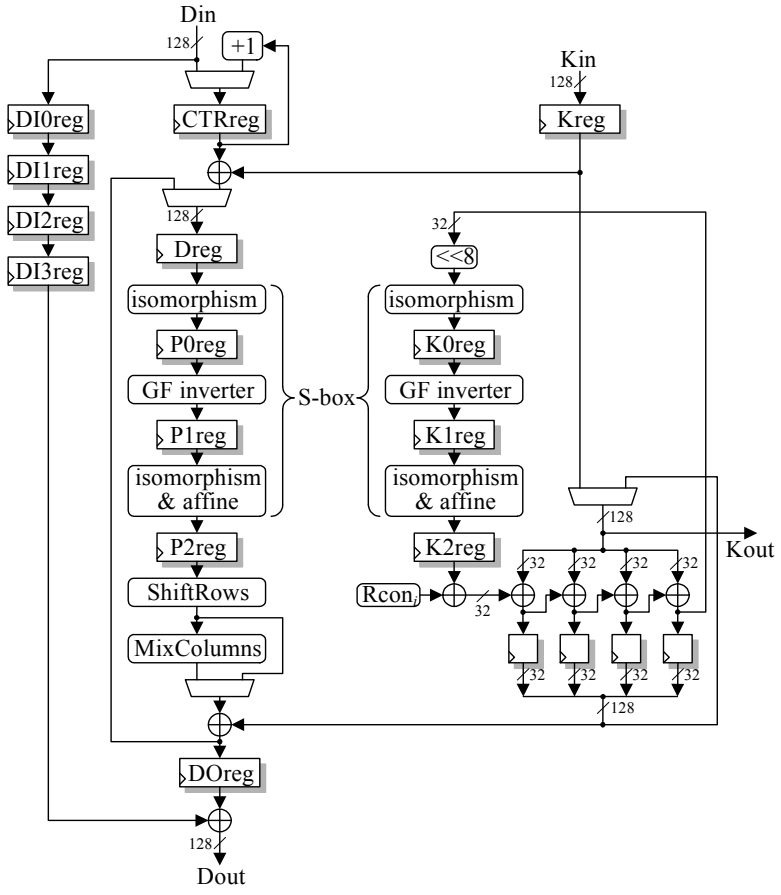


図 5.6 AES5 のデータパス

図 5.7 に最短サイクルでの暗号化および復号処理のタイミングチャートを示す. なお，これら処理中は START=1 に固定されている.

CLK1: RSTn=0 とすることで，制御回路がリセットされる．

CLK2: Krdy=1 とすることで，入力ポート Kin 上の 128bit の秘密鍵 Key が鍵レジスタ Kreg にストアされる．

CLK3: CTRrdy=1 とすることで，入力ポート Din 上の 128bit のカウンタ値 Ctr が，カウンタレジスタ CTRreg にセットされる．最初のラウンド鍵 Kr0 は秘密鍵 Key と同一である．

CLK4: 疑似乱数生成が開始され，ビジー信号 BSY=1 となる．データ入力許可信号 Drcv=1 なので，BSY=1 であるがデータ入力レジスタに空きがあり，平文(または暗号文)が入力可能であることがわかる．そこで，Drdy=1 とすることで，データ入力ポート Din 上の平文ブロック Pt0 をデータ入力レジスタにラッチしている．この平文ブロックは後に疑似乱数生成が完了した段階で暗号化されて出力される．

CLK5-7: 続く 3 クロックで 3 つの平文ブロック Pt1~Pt3 をストアしている．

CLK8: 4 つ全ての 128bit データ入力レジスタに平文ブロックがストアされたので，これ以上データが入力できないことを知らせるため，データ入力許可信号 Drcv=0 となる．2 番目のラウンド鍵 Kr1 が鍵出力ポート Kout から出力される．これ以降，4 クロック毎に，ラウンド鍵 Kr2~Kr10 が順番に出力されていく．

CLK46: 乱数生成が完了し，BSY=0 となる．それと同時に最初の 128bit の暗号文データブロック Ct0 がデータ出力ポート Dout に出力され，データ有効信号 Dvld=1 となる．

CLK47~49: 続いて 3 つの暗号文ブロック Ct1~Ct3 が順番に出力される．このように 4 つの暗号文ブロックがセットで一度に出力されるため，3 つの平文ブロックがデータ入力レジスタにセットされていても，あと 1 ブロック入力されるまでは，暗号文ブロックの出力はない．従って，入力データブロック数が 4 の倍数でないときは，暗号文を押しだすために，ダミーのブロックを入力する必要がある．

CLK50: データ入力レジスタの 4 つ全ての平文ブロックが疑似乱数と XOR され，暗号文として出力された後，Dvld=0 となる．4 つの暗号文が出力されると，直ちに次の乱数生成処理が始まり，BSY=1 となる．また，データ入力許可信号 Drcv=1 となったので，Drdy=1 とすることで次のデータ入力ポート Din 上の平文ブロック Pt4 をストアする．

CLK51: 平文ブロック Pt4 は Din 上にアサインされているが，Drdy=0 なのでこのクロックで 2 ブロック目のデータとしてストアされることはない．

CLK52-53: Drdy=1 としたことで，続く 2 ブロックの平文 Pt5 と Pt6 がストアされる．

CLK54: Drdy=0 から平文ブロックのストアは行われない．

CLK55: Drdy=1 から平文ブロック Pt7 がストアされる．

CLK56: 4 つの連続する平文ブロックがストアされたので，Drcv=0 となる．

CLK92~95: 前回，暗号文出力のあった CLK46~CLK49 から最短の 46 クロック後に，4 ブロックの暗号文 Ct4~Ct7 が連続して出力される．

CLK96: Drcv=1 となるが，この時点ではデータ入力は行われない．

CLK137: 乱数生成が完了し BSY=0 となるが，平文(または暗号文)の入力が行われていないため，当然それに対応する暗号文(または平文)の出力はない．BSY=0 の時に限り新しい鍵と，カウンタ値をセットすることが可能である．BSY=0 となるのを待たずに，直ちに新しい鍵とカウンタ値をセットしたいのであれば，RSTn=0 としてマクロ全体をリセットする必要がある．このクロック CLK137 では暗号文 Ct0~Ct3 を復号するために，CLK3 でセットしたカウンタ値と同じ Ctr をセットしている．鍵は新たに入力しないので，CLK2 でセットされたものがそのまま使われる．

CLK138: Drcv=1 なので，最初の暗号文ブロック Ct0 を入力する．

CLK139: 乱数生成が始まり BSY=1 となる．また，2 番目の暗号文ブロック Ct1 を入力する．

CLK140: 3 番目の暗号文ブロック Ct2 を入力する．

CLK179: 乱数生成が完了し BSY=0 となるが，暗号文は 3 ブロックしか入力されていないので，平文出力はまだ行われない．

CLK180: 4 番目の暗号文ブロック Ct3 が入力され，4 つのデータ入力レジスタ DI0reg~DI3reg が埋まったので，Drcv=0 となりこれ以上データ入力を受け付けなくなる．

CLK181~84: Dvld=1 となり 4 つの平文ブロック Pt0~Pt3 が順番に出力される.
CLK185: データ入力レジスタが空となったので Drcv=1 となり, また, 次の乱数生成が始まり BSY=1 となる.

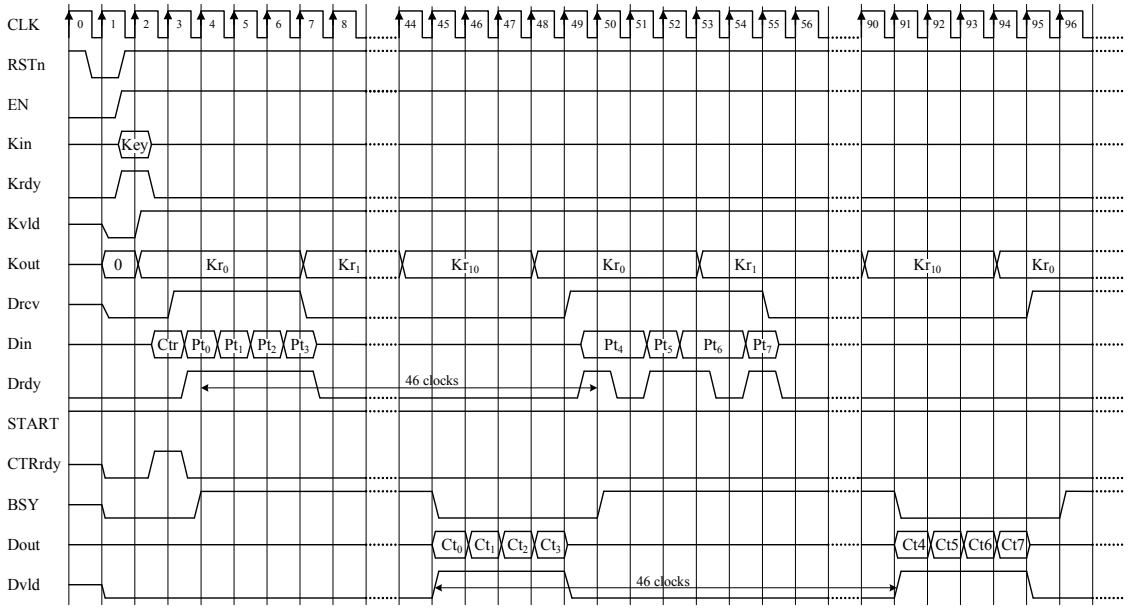


図 5.7-1 AES5 の暗号化・復号処理のタイミングチャート

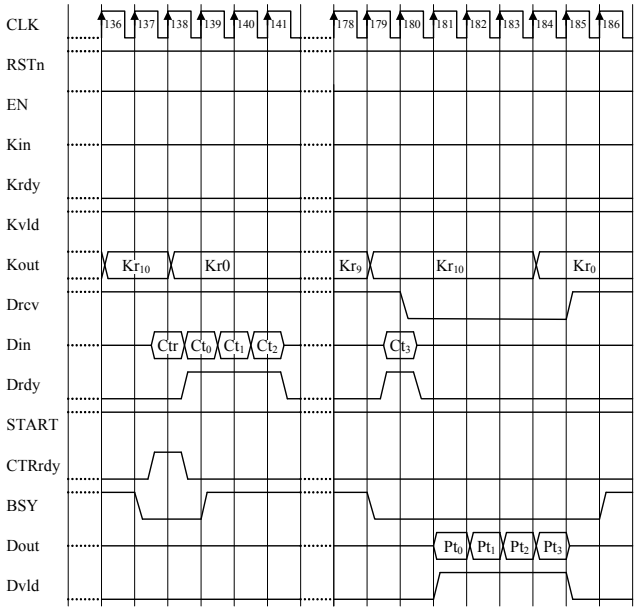


図 5.7-2 AES5 の暗号化・復号処理のタイミングチャート

図 5.8 は, START 信号を制御しながら暗号化(または復号)を行う場合のタイミングチャートである. 図 5.7 のように START=1 と固定されている場合は, 4 つの平文(または暗号文)ブロックが入力されると, AES コアが生成した乱数との XOR が行われて暗号文(または平文)が出力されるのと同時に, 自動的に AES コアにおいて次の乱数生成が開始される. しかし, サイドチャネル攻撃実験の電力・電磁波形測定には AES コアの動作開始を明示的に外部から指定する必要があるため, この START 信号が用意されている.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.
CLK2: Krdy=1 とすることで, 入力ポート Kin 上の 128bit の秘密鍵 Key が鍵レジスタ Kreg にスト

アされる.

CLK3: CTRrdy=1 とすることで, 入力ポート Din 上の 128bit のカウンタ値 Ctr が, カウンタレジスタ CTRreg にセットされる. 最初のラウンド鍵 Kr0 は秘密鍵 Key と同一である.

CLK4: 疑似乱数生成が開始され, ビジー信号 BSY=1 となる. データ入力許可信号 Drcv=1 であるが, 図 5.7 とは異なりこのクロックでの平文入力は行われない.

CLK46: 乱数生成が完了し, BSY=0 となる. それと同時に最初の 128bit の平文ブロック Pt0 が入力されるが, AES コアは 4 ブロックの平文がそろうまでアイドル状態となる. このクロックで START=1 としているが, 平文がそろっていないので, これは意味をなさない.

CLK48-49: 2 番目と 3 番目の平文ブロック Pt1 と Pt2 が入力される.

CLK51: 4 番目の平文ブロック Pt3 が入力される. .

CLK52: データ入力レジスタがいっぱいになったので, データ入力許可信号 Drcv=0 となる.

CLK53~56: 4 つの平文ブロック Pt0~Pt3 に対応する暗号文ブロック Ct0~Ct3 が順番に出力される.

CLK56: 次の乱数生成に備えるため, ラウンド鍵が Kr10 から Kr0 にリセットされる.

CLK99: 復号に備え, BSY=0 の間にカウンタレジスタの値を初期値 Ctr にセットしなおす.

CLK100: ラウンド鍵出力が Kr0 となる.

CLK101: 乱数生成が開始され BSY=1 となる.

CLK142: 乱数生成が完了し BSY=0 となる. この時点でまだ平文ブロックは入力されていないので, AES コアはアイドル状態となる.

CLK144~147: Drdy=1 として, 4 つの暗号文ブロック Ct0~Ct3 をセットする.

CLK148: データ入力レジスタが暗号文で埋まったので Drcv=0 となる.

CLK149~152: 4 つの平文ブロック Pt0~Pt3 が出力される.

CLK152: 次の乱数生成処理に備えてラウンド鍵レジスタ出力が Kr0 にリセットされるが, START=0 となっているため, その処理はまだ開始されない.

CLK153: 4 つの平文ブロックが出力された結果データ入力レジスタが空となり, Drcv=1 となる.

CLK154: START=1 としたことで, 乱数生成が開始される.

CLK156: 乱数生成が始まったことで BSY=1 となる. .

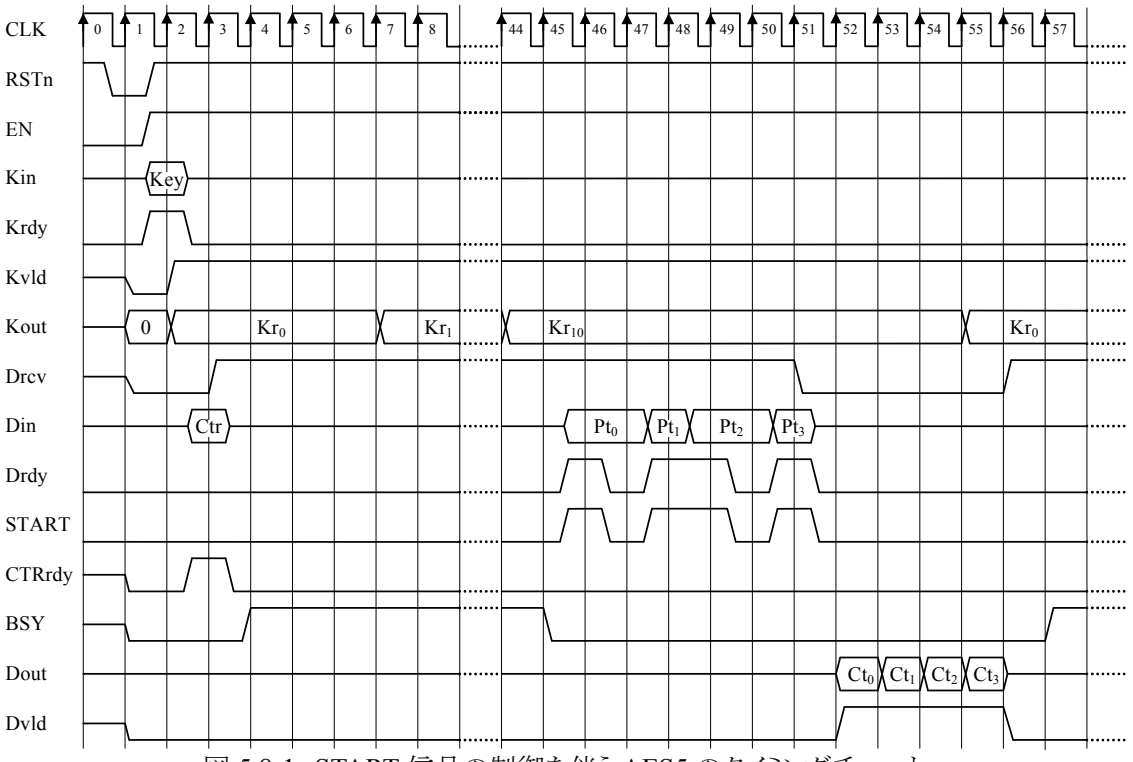


図 5.8-1 START 信号の制御を伴う AES5 のタイミングチャート

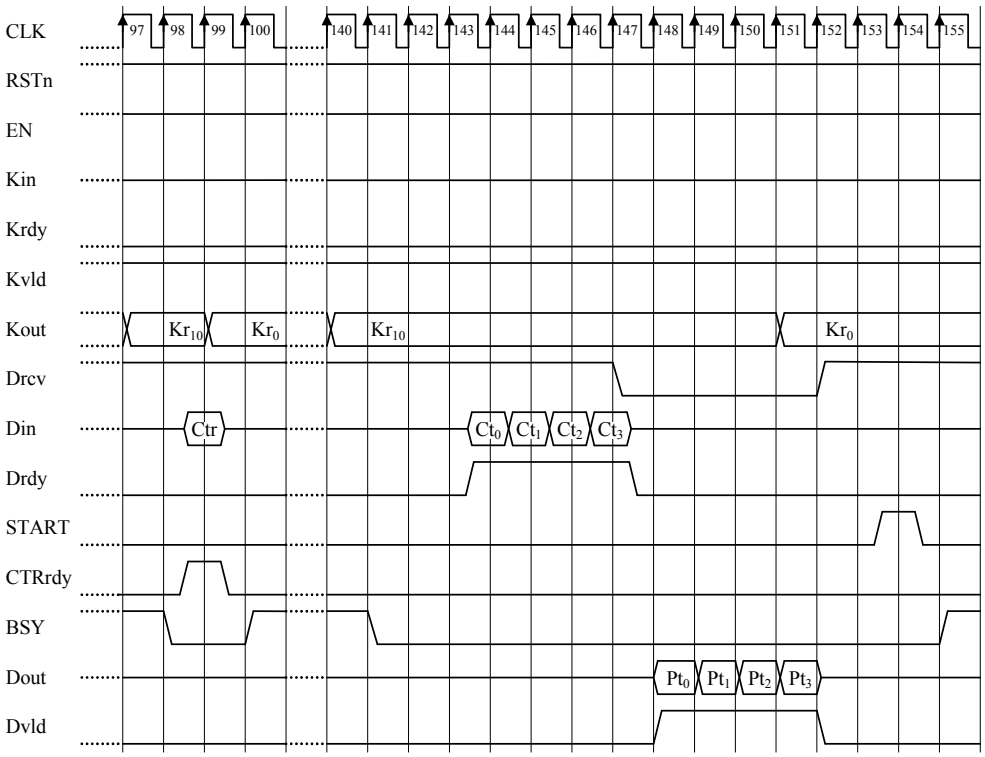


図 5.8-2　START 信号の制御を伴う AES5 のタイミングチャート

5.4　AES6 (FA 対策版)

故障利用解析攻撃(FA:Fault injection Attack)対策を施した暗号回路マクロ AES6 の概要と I/O ポートを，それぞれ表 5.7 と表 5.8 に示す．本マクロは暗号化(または復号)における中間値を 1/2 ラウンド単位でチェックし，復号(または暗号化)して正しく 1/2 ラウンド前の値に戻るかどうかを調べている．また，鍵データにもエラーがないか最終ラウンド鍵をチェックしている．

表 5.7　AES6 の概要

アルゴリズム	AES
データブロック長	128 bits
鍵長	128 bits
機能	暗号化/復号，エラー検出
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	AES_FA.v
記述言語	Verilog-HDL
トップモジュール名	AES
S-box	合成体 GF(((2^2)^2)^2)ベース
スループット	128 bit / 21 clock
ラウンド鍵生成	On-the-fly

表 5.8 AES6 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 128bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 AES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.
Err	Out	2	Err[0]=0: データエラーなし =1: データエラー発生 Err[1]=0: 鍵エラーなし =1 鍵エラー発生

図 5.9 に示す AES6 のベースとなるアーキテクチャでは, S-box 内のガロア体 GF(2^8)の逆元演算器や, マトリクス乗算である MixColumns と InvMixColumns の共通項の共有化を行っている. 通常はこの図のようにコンポーネント共有のため, 復号で AddRoundKey と InvMixColumns(図 5.9 では InvMixCol.と表示)の順番を入れ替え, かつそのつじつまを合わせるために右半分の鍵スケジューラのラウンド鍵出力に MixColumns を施す. しかしながら, 後で説明するように本マクロではこのような関数の順序の変更は行わない.

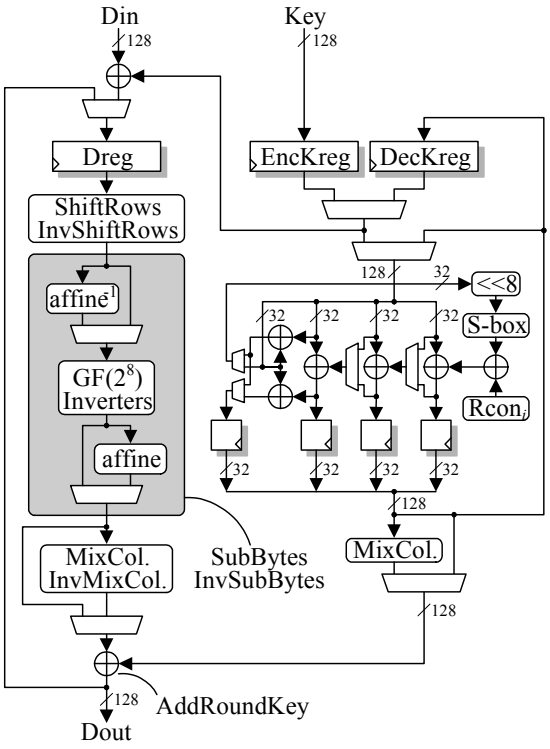


図 5.9 暗号化と復号でコンポーネントを共有する AES のデータパスアーキテクチャ

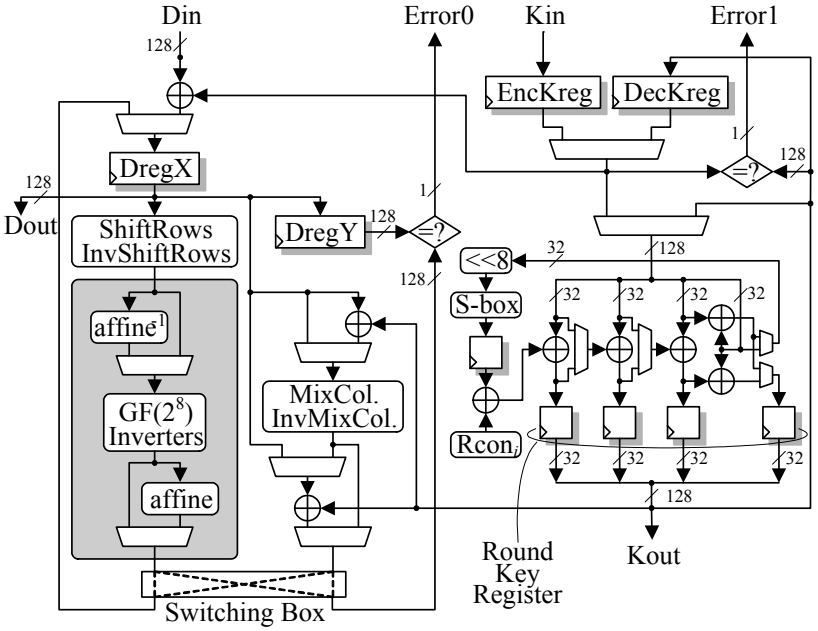


図 5.10 故障利用解析攻撃対策版 AES 暗号化・復号回路

図 5.10 は故障利用解析攻撃対策を施したマクロ AES6 のデータパスを示しており，暗号化と復号でデータパスを共有した上，ラウンド関数を 2 分割してその一方を暗号化（または復号）に使用し，他方でエラー検出のための復号（または暗号化）を行うものである．なお，図 5.9 のアーキテクチャのように AddRoundKey と InvMixColumns の順序を入れ替えて XOR ゲートを共有することを行っていない．XOR ゲートの共有でラウンド関数ブロックのクリティカルパスを短縮できるが，その代わりに鍵スケジューラに MixColumns が必要となる．これに対してラウンド関数を 2 分割する本方式では，XOR を共有せずに鍵スケジューラの MixColumns を省略したほうが回路規模と動作速度のバラン

スが良くなる. なおラウンド関数ブロックの分割に加えて, 鍵スケジューラもクリティカルパスとならないように 2 分割してレジスタを挿入し, 1 ラウンドを 2 クロックで処理している. ラウンド関数は正しく動作していても, 鍵スケジューラにエラーが発生したり, 制御カウンタの故障によって本来 10 ラウンドの繰り返し処理が 1 回で終了してしまうことなどが考えられる. これを防ぐために, 最終ラウンドの処理が終了したときに on-the-fly で生成された鍵を調べ, 暗号化であれば復号鍵レジスタ(DecKreg)と, 復号であれば暗号化鍵レジスタ(EncKreg)との一致を確認している. 攻撃者がカウンタの値を飛ばすことができたとしても, 値が不明の鍵スケジューラの 128bit まで正しく飛ばすことは不可能である.

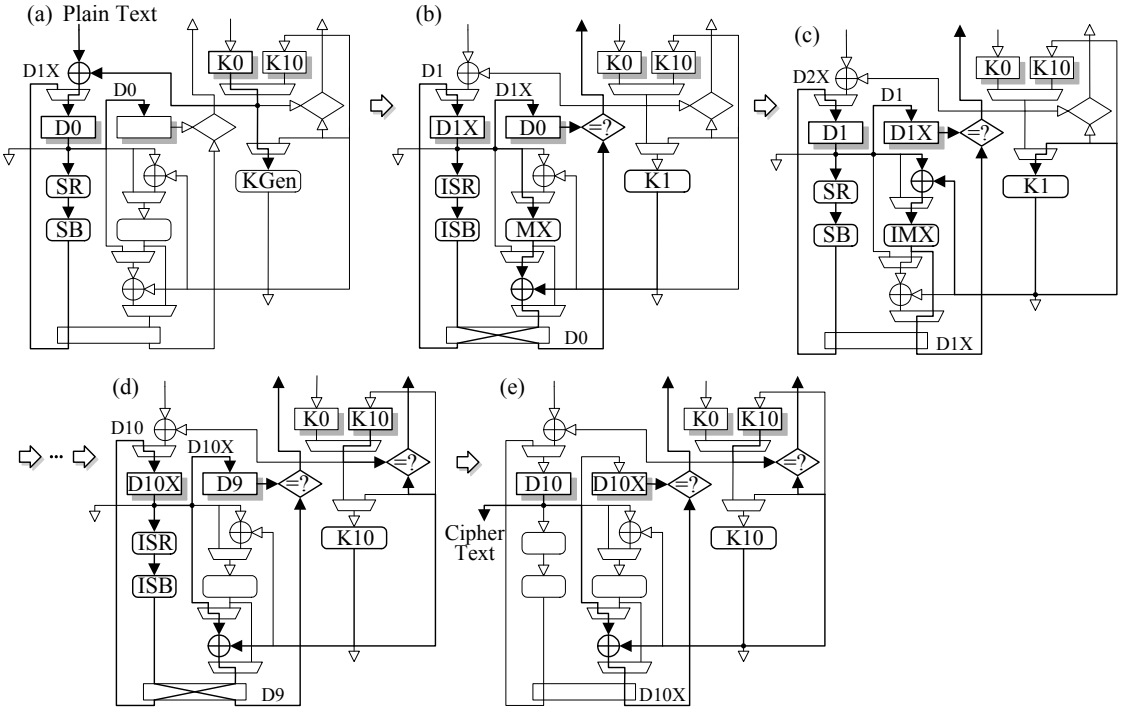


図 5.11 故障利用解析攻撃対策版回路の暗号化動作例

図 5.11 に暗号化処理の動作例を示す. 暗号化用の初期鍵 K0 はレジスタ EncKreg に入力され, 右側の鍵スケジューラで復号用の初期鍵(=暗号化用の最終鍵)K10 に変換されて DecKreg に既にセットされているものとする. まず(a)では, 入力された平文と暗号化用の初期鍵 K0 が XOR されてレジスタ DregX に D0 として書き込まれ, 暗号化処理の前半の ShiftRows と SubBytes のパスを通ったデータが D1X としてフィードバックされる. それと同時にデータ D0 は DregY に渡される. また鍵スケジューラでは, on-the-fly で初期鍵 K0 から第 1 ラウンドの鍵 K1 が生成される. (b)では検算のために(a)で暗号化に使用したパスで復号が行われ, DregX に書き込まれたデータ D1X を InvShirtRows と InvSubBytes によって逆変換の後, DregY に保持されている値 D0 と比較される. 一方, 同じデータ D1X は別のパスで MixColumns と AddroundKey(ラウンド鍵 K1 との XOR)により D1 に変換される. (c)では(a)と同じパスでレジスタ DregX の値 D1 が D2X に変換されるのと同時に, その右のパスの InvMixColumns と XOR で D1X に戻されてレジスタ DregY の値と比較される. 以下同様に, 第 9 ラウンドまで暗号化と検算が繰り返される. (d)ではエラー検出のために InvShiftRows と InvSubBytes, そして暗号化の最後の処理である最終第 10 ラウンドの鍵 K10 との XOR が行われる. 最終ラウンドでは MixColumns は行われないので, その処理ブロックはバイパスされる. 最終ラウンドなので, オンザフライで生成されたラウンド鍵レジスタの K10 と事前計算による EncKreg の K10 との比較により, 10 ラウンドきちんと処理されたことのチェックが行われる. ここで暗号文 D10 の出力も可能であるが, 最後に(e)で D10X に戻ることが確認された後に出力している. この最終チェックが済むまで次の平文は入力されないため, 1 ブロックの暗号化に要するクロック数は, 20 クロック(=10 ラウンド×2 クロック)に(e)の 1 クロック分が加算され, 21 クロックとなる.

5.5 AES7 (ラウンド鍵事前生成)

AES 暗号回路マクロ AES7 はラウンド鍵の事前計算を行って 128bit×11 のレジスタに保持するという点が, On-the-fly でラウンド鍵を生成する他の AES マクロと異なっている. 本マクロの概要を表 5.9 に, I/O ポートを表 3.10 に示す.

表 5.9　AES7 の概要

アルゴリズム	AES
データブロック長	128 bits
鍵長	128 bits
機能	暗号化のみ
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	AES_PreKeyGen.v
記述言語	Verilog-HDL
トップモジュール名	AES_PKG
S-box	合成体 GF(((2^2)^2)^2)
スループット	128 bit / 10 clock
ラウンド鍵生成	事前計算

表 5.10　AES7 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき,秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, 平文データが 内部レジスタにラッチされ, 暗号化処理が開始される.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 AES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化あるいは鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化が実行可能となる.
Dvld	Out	1	暗号化処理が完了し, 暗号文がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

図 5.12 に AES7 のデータパスアーキテクチャを示す. 図 5.1 の AES0 の暗号化回路に, ラウンド鍵保存用の 128bit×11 のレジスタが付加された構造をしている. 秘密鍵が Kin から入力されると, 鍵スケジュールが行われてラウンド鍵がこのレジスタに保存される. 暗号化時にはこのレジスタから AddRoundKey へ鍵が出力されるので, 鍵スケジューラは動作しない.

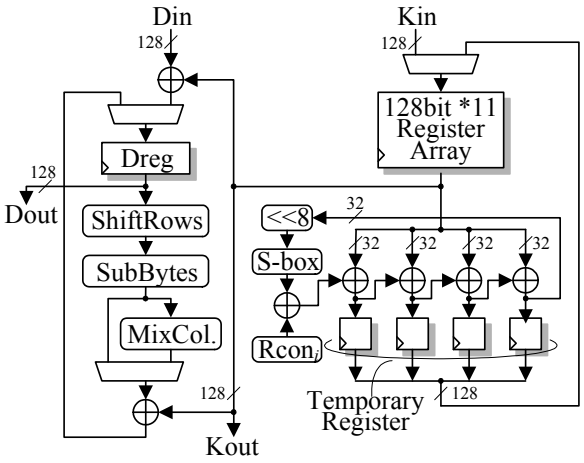


図 5.12 AES7 のデータパスアーキテクチャ

図 5.13 に最短サイクルでの暗号化処理のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.

CLK2: Krdy=1 とすることで, 128bit ポート Kin に入力された秘密鍵が内部レジスタにセットされる.

CLK3: 鍵スケジュール処理が開始され, ビジーフラグ BSY=1 となる. この間に Krdy=0 とされる.

CLK14: 鍵スケジュール処理が完了し, BSY=0 となり, また鍵が有効になったことを示すフラグ Kvld=1 となる.

CLK15: このクロックから平文入力して暗号化を行うことが可能となる. Drdy=1 とすることで 128bit ポート Din 上の平文 Pt0 が鍵レジスタから出力される最初のラウンド鍵 Kr0(入力された秘密鍵 Key と同じ)と XOR されてデータレジスタ Dreg にストアする. Kr0 は 128bit ポート Kout から出力される.

CLK16: 暗号化処理が開始され, BSY=1 となる. 2 番目のラウンド鍵 Kr1 が Kout から出力されるのと同時に, Dreg の途中結果が 128bit ポート Dout から出力される. このように暗号化処理の間, ラウンド鍵と途中結果が毎クロック出力される.

CLK17~26: 暗号化処理は 10 クロックを要し, CLK25 で完了する. CLK26 で BSY=0, Dvld=1 となり, 暗号文が Dout から出力される. この CLK26 に, 新しい平文 Pt1 を入力することが可能である.

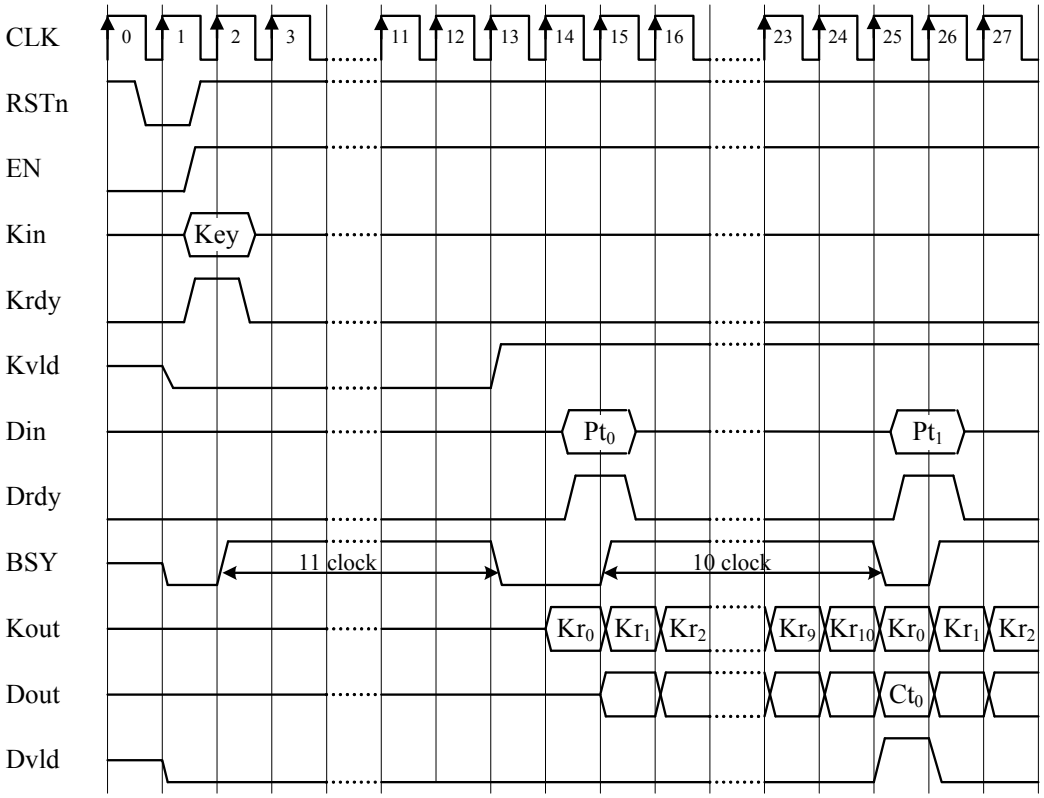


図 5.13　AES7 の暗号化のタイミングチャート

5.6　AES8（MAO）

AES8 は Trichina らによって提案された乱数マスクによる DPA 対策方式，Masked-AND Operation (MAO)[6]を実装している．図 5.14 は Masked-AND の基本ゲート構成を示している．真のデータ<a, b>は互いに独立な乱数 <m_a, m_b>によって XOR マスクされ，<$\tilde{a}$, $\tilde{b}$ >として入力される．そして，a と b の論理積 $a \bullet b$ を新たな独立な乱数入力 m でマスクした値 $(a \bullet b) \oplus m$ が出力される．真に行いたい演算の入力<a, b>も出力 $a \bullet b$ も，演算の途中で現れることはない．しかし，信号遅延のばらつきで生じるグリッチによる消費電力に秘密情報が漏洩する危険性の指摘もある．

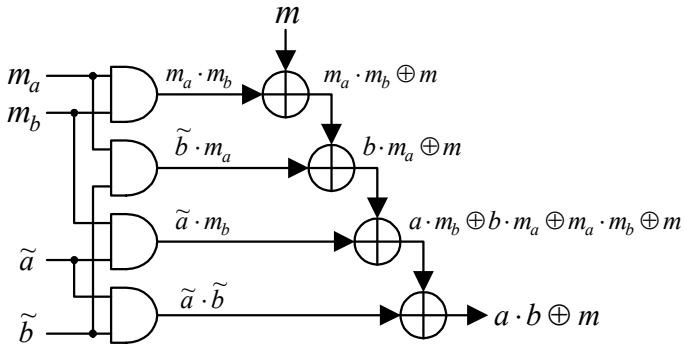


図 5.14　Masked-AND ゲート

5.7 AES9 (MDPL)

AES9はPopp らの提案によるDPA対策方式である，後述のWDDL[9]に乱数を組み合わせたMasked Dual-rail Precharge Logic (MDPL)[8]を実装している．図5.15にMDPLの基本構成を示す．図5.15(a)のMAJゲートは，3入力のうち0か1の多い方のビットを出力する多数決論理である．(b)のMDPL-ANDゲートは，MAJゲートを2つ相補的に配置することで，マスクされた入力 a_m , b_m と，マスク m（そしてそれらの反転した値）に対して次式の演算を行う．MDLP-ANDゲートの真理値表を表5.11に示しておく．

$$\begin{cases} q_m = MAJ(a_m, b_m, m) = MAJ(a \oplus m, b \oplus m, m) = a \cdot b \oplus m \\ \overline{q}_m = MAJ(\overline{a}_m, \overline{b}_m, \overline{m}) = MAJ(a \oplus \overline{m}, b \oplus \overline{m}, \overline{m}) = a \cdot b \oplus \overline{m} \end{cases}$$

WDDLでは相補的な配線の容量が等しくなければならないが，MDPLは図5.15(c)のように乱数 m（および $\overline{m}$ ）の値に応じてMAJ ゲートの出力がランダムに遷移するため，相補的な配線容量が釣り合っていない場合でも消費電力が均一化される．しかしながら，MDPLはWDDLに対して情報漏洩量は少ないものの，完全に隠すことはできないことが指摘されている．

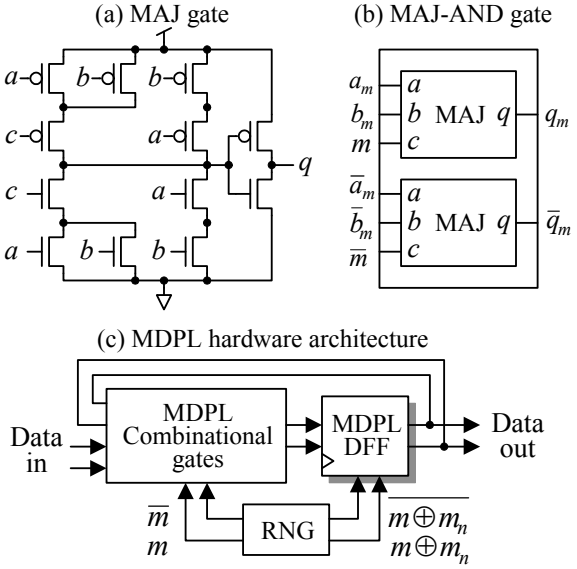


図 5.15 Masked Dual-rail Precharge Logic

表 5.11 MDPL-AND ゲートの真理値表

a	b	m	a_m	b_m	q_m	$\overline{m}$	$\overline{a}_m$	$\overline{b}_m$	$\overline{q}_m$
0	0	0	0	0	0	1	1	1	1
0	0	1	1	1	1	0	0	0	0
0	1	0	0	1	0	1	1	0	1
0	1	1	1	0	1	0	0	1	0
1	0	0	1	0	0	1	0	1	1
1	0	1	0	1	1	0	1	0	0
1	1	0	1	1	1	1	0	0	0
1	1	1	0	0	0	0	1	1	1

5.8 AES10 (Threshold Implementation)

AES10 は Nikova らによって提案された複数の乱数マスクを用いる DPA 対策方式, Threshold implementation[7)]を実装している. GF(2^m)上の加算を⊕, 総和を$\bigoplus$で表し, 入力変数 $x = \bigoplus_{i=1}^{n} x_i$ および $y = \bigoplus_{i=1}^{n} y_i$, 出力変数 $z = \bigoplus_{i=1}^{n} z_i$ とする.

$$\begin{cases} z_1 = (x_3 \oplus x_4)(y_2 \oplus y_3) \oplus y_2 \oplus y_3 \oplus y_4 \oplus x_2 \oplus x_3 \oplus x_4 \\ z_2 = (x_1 \oplus x_3)(y_1 \oplus y_4) \oplus y_1 \oplus y_3 \oplus y_4 \oplus x_1 \oplus x_3 \oplus x_4 \\ z_3 = (x_2 \oplus x_4)(y_1 \oplus y_4) \oplus y_2 \oplus x_2 \\ z_4 = (x_1 \oplus x_2)(y_2 \oplus y_3) \oplus y_1 \oplus x_1 \end{cases}$$

これらの基本構成要素式は以下の特性を満たしている.

1. どの関数も入力変数 x, y それぞれにおいて少なくとも 1 要素(x_n, x_n) と独立している.

$$z_n = f(x_1, x_2, \cdots, x_{n-1,} y_1, y_2, \cdots, y_{n-1,})$$

2. 出力要素の合計は元の出力を与える.

$$z = \bigoplus_{i=1}^{n} z_i = \bigoplus_{i=1}^{n} f_i(\cdots) = N(x)$$

3. 入力信号 x, y の全ての分配に対して, $z = N(x, y, ...)$ が実現できるならば, 次式は一定となる.

$$\Pr(\bar{z} = \overline{Z} \mid z = \bigoplus_{i=1}^{n} Z_i)$$

以上より, 入力変数は z_i と相関がない. すなわち, 演算処理が入力変数, 出力変数に依存していないことを示す. そして, 特性 3 で各要素に対するそれぞれの関数出力の遷移確率が一定であるということが示されているため, サイクル毎の消費電力が一定である. よって, 例えグリッチによる消費電力が発見されても秘密情報がリークするものではないという観点からも DPA 対策として有効である.

5.9 AES11 (WDDL)

AES11 は Tiri らによって提案された DPA 対策方式, Wave Dynamic Differential Logic (WDDL) [9)]を実装している. 図 5.16 は WDDL の基本構成要素を示しており, ゲートスイッチング時の消費電力を一定にすることを目的に 2 線ロジックの Sense Amplifier Based Logic (SABL) を応用している. データ入力回路ロジックのプリチャージ信号が 1 のとき, 組合せ回路への入力データは全て 0 に落とされ休止状態となる. そしてプリチャージ信号を 0 にすると, 入力データとして各データ入力ロジックから(0, 1)または(1, 0)の相補信号が組合せ回路に送られ, 演算が開始される. 組合せ回路全体のスイッチング回数は入力データ値に依存しないためほぼ一定の消費電力となり, 電力解析攻撃に有効であるとされる. しかし厳密には, AND ゲートと OR ゲートの消費電力には差があり, データ線ペアの配線容量の調節も必要である. そのため, WDDL ゲートの入出力信号の遅延のばらつきが, 秘密情報の漏洩を起こすことが指摘されている.

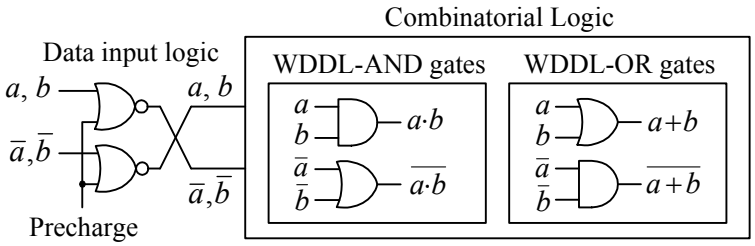


図 5.16 Wave Dynamic Differential Logic

3.10 AES12/AES13 (疑似 RSL)

Random Switching Logic (RSL) [10]は，三菱電機によって提案された出力許可信号付きの多数決論理ゲートを用いたトランジスタレベルの対策法である．図5.17はRSL によるNANDゲートを示しておいる．信号の遅延時間を考慮しない単純な乱数マスク対策では，過渡遷移から情報が漏洩する可能性があるため，RSL ゲートでは入力(x_z, y_z)，出力イネーブル($\overline{en}$)，そして乱数マスク(r_z)の信号遅延時間を制御して過渡遷移を防いでいる．また，リマスク処理をRSLゲート毎に行うことで，高次DPA等にも対策が可能となる．以下に，RSL-NANDゲートの処理過程を示す．

入力: $\overline{en}$, $\begin{cases} x = a \oplus r_x \\ y = b \oplus r_y \end{cases}$, $\begin{cases} r_z \\ r_{xz} = r_x \oplus r_z \\ r_{yz} = r_y \oplus r_z \end{cases}$ 出力: $\overline{a \cdot b} \oplus r_z$

処理1: $\overline{en} = 1$ (過渡遷移抑制)

処理2: $\begin{cases} x_z = x \oplus r_{xz} (= a \oplus r_z) & (x\text{のリマスク}) \\ y_z = y \oplus r_{yz} (= b \oplus r_z) & (y\text{のリマスク}) \end{cases}$

処理3: $\text{RSL-NAND}(x_z, y_z, r_z, \overline{en})$ (RSL-NANDゲートへ入力データをセット)

処理4: $\overline{en} = 0$ (データ確定後に出力をイネーブル)

RSLゲートは専用セルが必要なため，通常のCMOSライブラリを用いて動作を模擬する方式が疑似RSLであり，AES12/AES13ではこの方式を実装している．図5.18は多入力AND-ORゲートを多数決論理に利用した疑似RSL-NANDで，後段のNORゲートは，過渡遷移の発生を擬似RSL内に止めて後段に伝播させないための出力制御に用いられる．

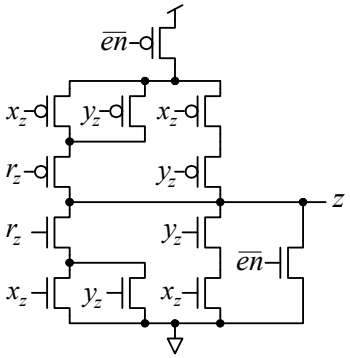


図 5.17 RSL-NAND ゲート

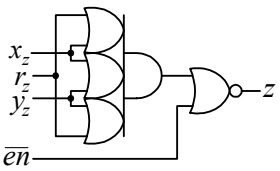


図 5.18 疑似 RSL-NAND ゲート

5.11 Camellia

Camellia[11]の暗号回路マクロ概要を表 5.12 に，I/O ポートを表 5.13 に示す．Camellia は Feistel 構造を持つブロック暗号であるため，AES よりも多くのサイクル数を要するが，暗号化と復号に同じ

データパスが使用できるため，単純実装では SPN 型の AES よりも小型実装に向いている．

表 5.12 Camellia の概要

アルゴリズム	Camellia
データブロック長	128 bits
鍵長	128 bits
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	Camellia.v
記述言語	Verilog-HDL
トップモジュール名	Camellia
S-box	テーブル実装
スループット	128 bit / 23 clock
ラウンド鍵生成	事前計算 & On-the-fly

表 5.13 Camellia の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき，Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ，鍵の初期化処理が開始される. もし Drdy と Krdy に同時に ‘1’ が入力された場合は，Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき，Din に入力された 128bit の平文(または暗号文)データが 内部レジスタにラッチされ，暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに，EncDec=0 ならば暗号化処理が，EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると，制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも，システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき，本暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは，このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは，暗号化/復号/鍵初期化処理が行われている間，1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると，1 クロックの間だけ Kvld=1 となり，次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し，暗号文(または平文)がデータ出力ポート Dout にセットされると，1 クロックの間だけ Dryd=1 となり，次のクロックですぐに 0 に落とされる.

Camellia のデータパスアーキテクチャを図 5.19 に示す. 1 ラウンドは 1 クロックで処理され, 128bit の平文または暗号文を暗号化または復号するのに, いずれも 23 クロックを要する. 秘密鍵が入力されると鍵レジスタ kl にラッチされた後, 図下側のデータランダム化部で初期変換がおこなわれてレジスタ ka にストアされる. ラウンド鍵はこの kl と ka から on-the-fly で作られる.

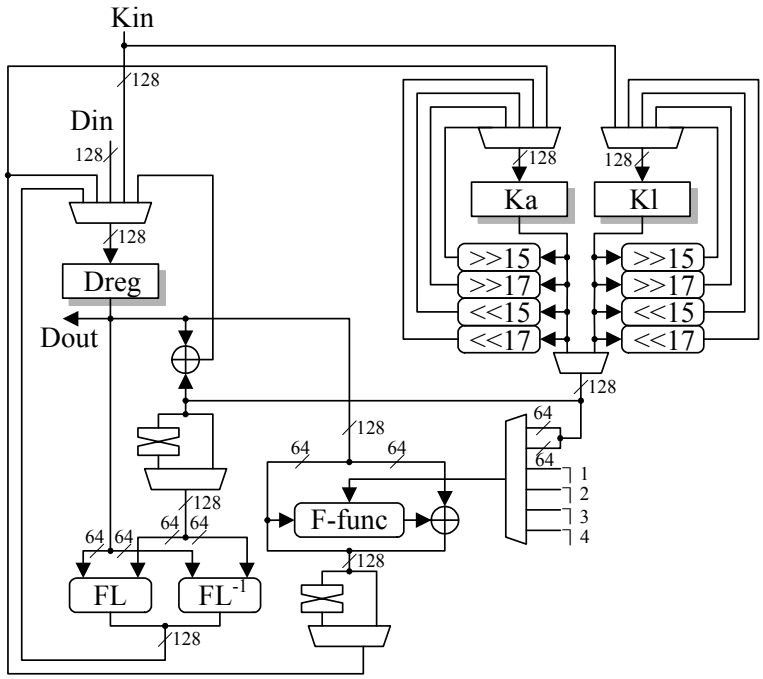


図 5.19 Camellia のデータパスアーキテクチャ

図 5.20 に最短サイクルでの鍵スケジュールと暗号化, 図 5.21 に復号のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.
CLK2: Krdy=1 とすることで, 128bit ポート Kin に入力された秘密鍵が内部レジスタにセットされる.
CLK3: 鍵スケジュール処理が開始され, ビジーフラグ BSY=1 となる. この間に Krdy=0 とされる.
CLK8: 鍵スケジュール処理が 8 クロックで完了し, BSY=0 となり, また鍵が有効になったことを示すフラグ Kvld=1 となる.
CLK9: このクロックから平文または暗号文入力が可能となる. EncDec=0(暗号化), そして Drdy=1 とすることで 128bit ポート Din 上の平文がデータレジスタ Dreg にストアされる.
CLK10: 暗号化処理が開始され, BSY=1 となる. Dreg の途中結果が 128bit ポート Dout から出力されるのと同時に, ラウンド鍵 Kw1,Kw2 が Kout から出力される. このように暗号化処理の間, 途中結果とラウンド鍵が毎クロック出力される.
CLK32: 暗号化処理が 23 クロックで終了し, BSY=0 となる. 暗号文が Dout から出力されるのと同時に Dvld がこのクロックで 1 となり, 次のクロックですぐに 0 に落ちる.
CLK33: Drdy=1 とすることで次の処理を開始する. ここでは復号を行うために EncDec=1 とし暗号文を 128bit ポート Din に入力する.
CLK34: 復号処理が開始され BSY=1 となる. 暗号化と同様に途中結果とラウンド鍵が毎クロック Dout と Kout から出力される.
CLK57: 復号が 23 クロックで完了し BSY=0 となる. 平文が Dout から出力され, Dvld がこのクロックだけ 1 となる.

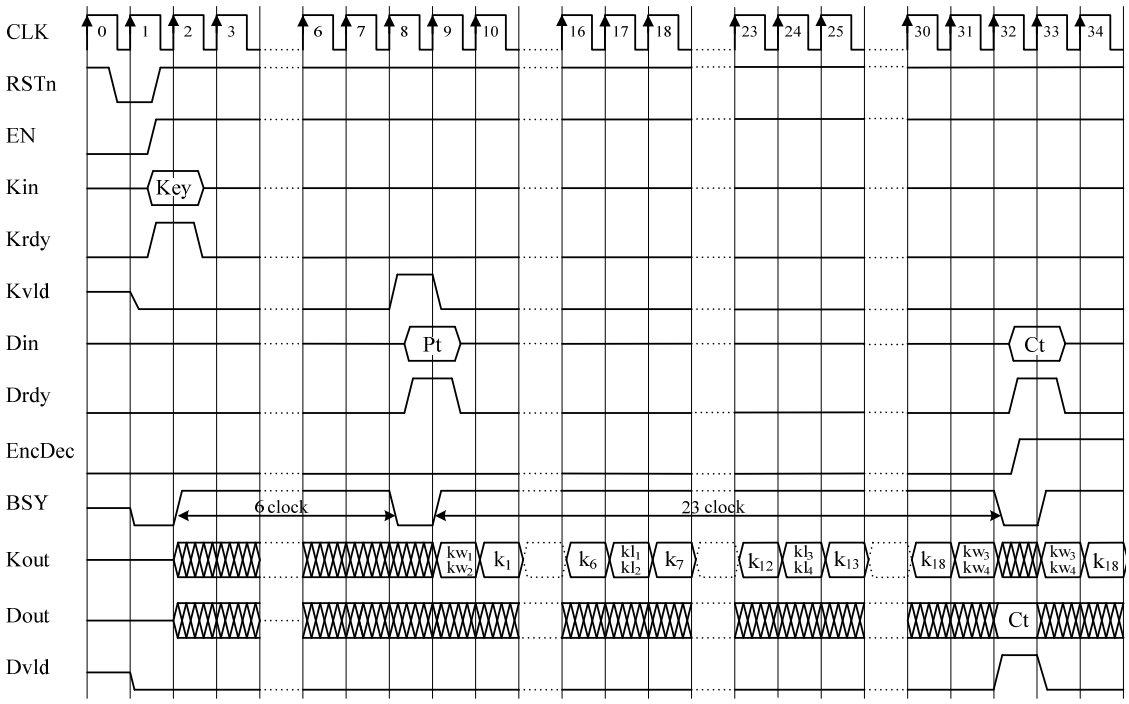


図 5.20 Camellia の鍵スケジュールと暗号化のタイミングチャート

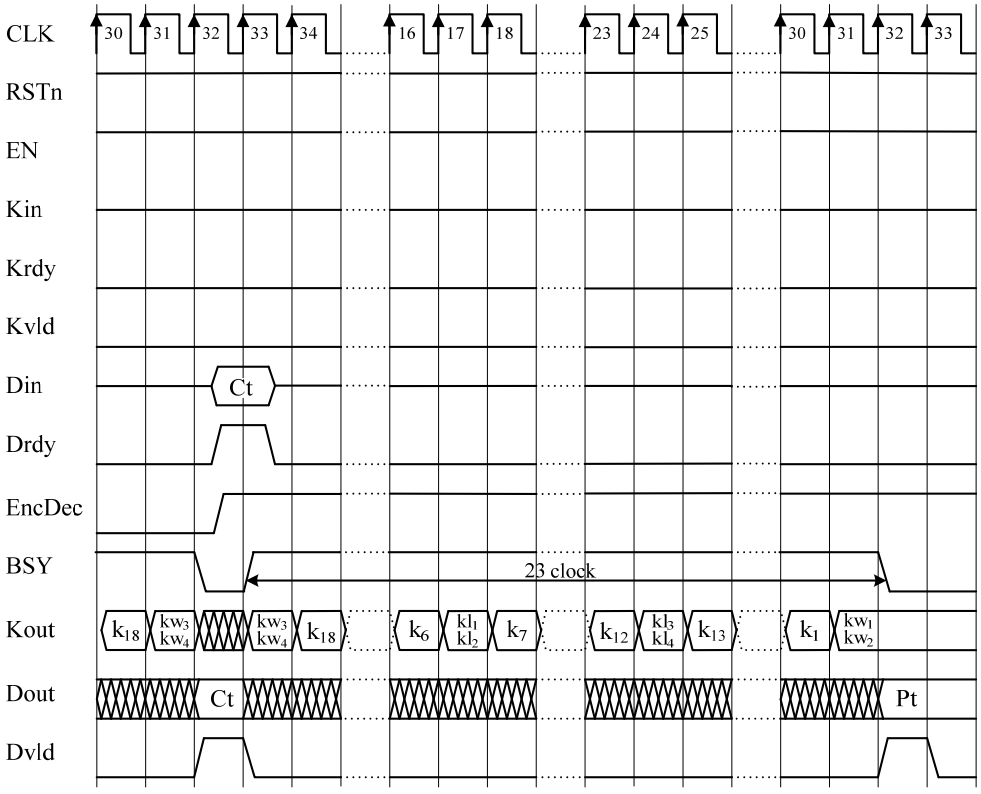


図 5.21 Camellia の復号タイミングチャート

5.12 CAST-128

CAST-128[12]はデータ長 64bit, 鍵長 128bit のブロック暗号である. CAST-128 の暗号回路マクロ概要を表 5.14 に, I/O ポートを表 5.15 に示す.

表 5.14 CAST-128 の概要

アルゴリズム	CAST-128
データブロック長	64 bits
鍵長	128 bits
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	CAST128.v
記述言語	Verilog-HDL
トップモジュール名	CAST
S-box	テーブル実装
スループット	64 bit / 17 clock
ラウンド鍵生成	事前計算

表 5.15 CAST-128 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力. 意味のあるのは下位の Kr_i(5bit)と Km_i(32bit)の 37bit で, 上位 91bit は 0 でパディングされる.
Din	In	64	データ入力.
Dout	Out	64	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 64bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

CAST-128 のデータパスアーキテクチャ [13]を図 5.22 に示す. Feistel 構造を持つブロック暗号で 32bitプロセッサ上でのソフトウェアには向いているものの, ランダムテーブルで記述された 8 種類の 8bit 入力/32bit 出力の S-box や, 32bit 加減算器が必要となるため, 回路規模は大きい. また 1 ラウンド/クロックで処理するには, ラウンド鍵を事前計算しておく必要があり, 鍵スケジュール部に大きなラウンド鍵用レジスタが付加されている. 2 つのラウンド鍵 Kr_i は 5bit, Km_i は 32bit なので, これらを外部の 128bit ポート Kout に出力する際には, 上位 91bit に 0 をパディングし, Kr_i と Km_i を連接する.

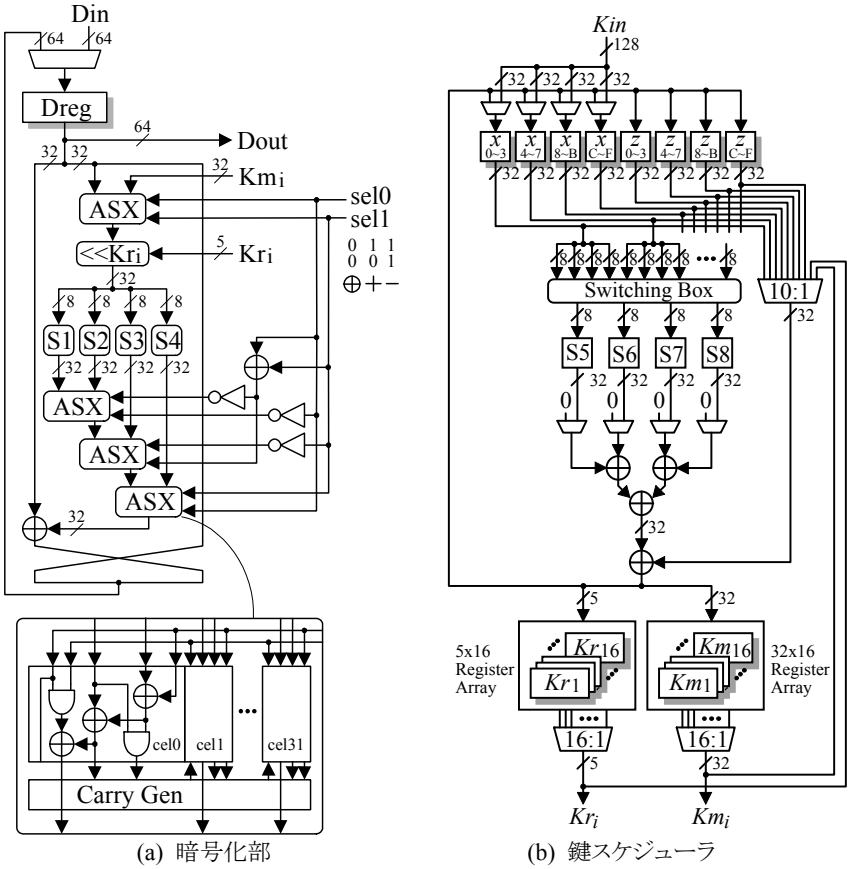


図 5.22 CAST-128 のデータパスアーキテクチャ

図 5.23 に最短サイクルでの鍵スケジュール, 暗号化, そして復号処理のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.
CLK2: Krdy=1 とすることで, 128bit ポート Kin に入力された秘密鍵が内部レジスタにセットされる.
CLK3: 鍵スケジュール処理が開始され, ビジーフラグ BSY=1 となる. この間に Krdy=0 とされる.
CLK130: 鍵スケジュール処理が 128 クロックで完了し, BSY=0 となり, また鍵が有効になったことを示すフラグ Kvld=1 となる.
CLK131: このクロックから平文または暗号文入力が可能となる. EncDec=0(暗号化), そして Drdy=1 とすることで 64bit ポート Din 上の平文がデータレジスタ Dreg にストアされる.
CLK132: 暗号化処理が開始され, BSY=1 となる. Dreg の途中結果が 64bit ポート Dout から出力されるのと同時に, ラウンド鍵 Kr_i と Km_i が Kout から出力される. このように暗号化処理の間, 途中結果とラウンド鍵が毎クロック出力される.
CLK148: 暗号化処理が 16 クロックで終了し, BSY=0 となる. 64bit の暗号文が Dout から出力されるのと同時に Dvld がこのクロックで 1 となり, 次のクロックですぐに 0 に落ちる.
CLK149: Drdy=1 とすることで次の処理を開始する. ここでは復号を行うために EncDec=1 とし暗号

文を 64bit ポート Din に入力する.

CLK150: 復号処理が開始され BSY=1 となる. 暗号化と同様に途中結果とラウンド鍵が毎クロック Dout と Kout から出力される.

CLK165: 復号が 163 クロックで完了し BSY=0 となる. 64bit の平文が Dout から出力され, Dvld がこのクロックだけ 1 となる.

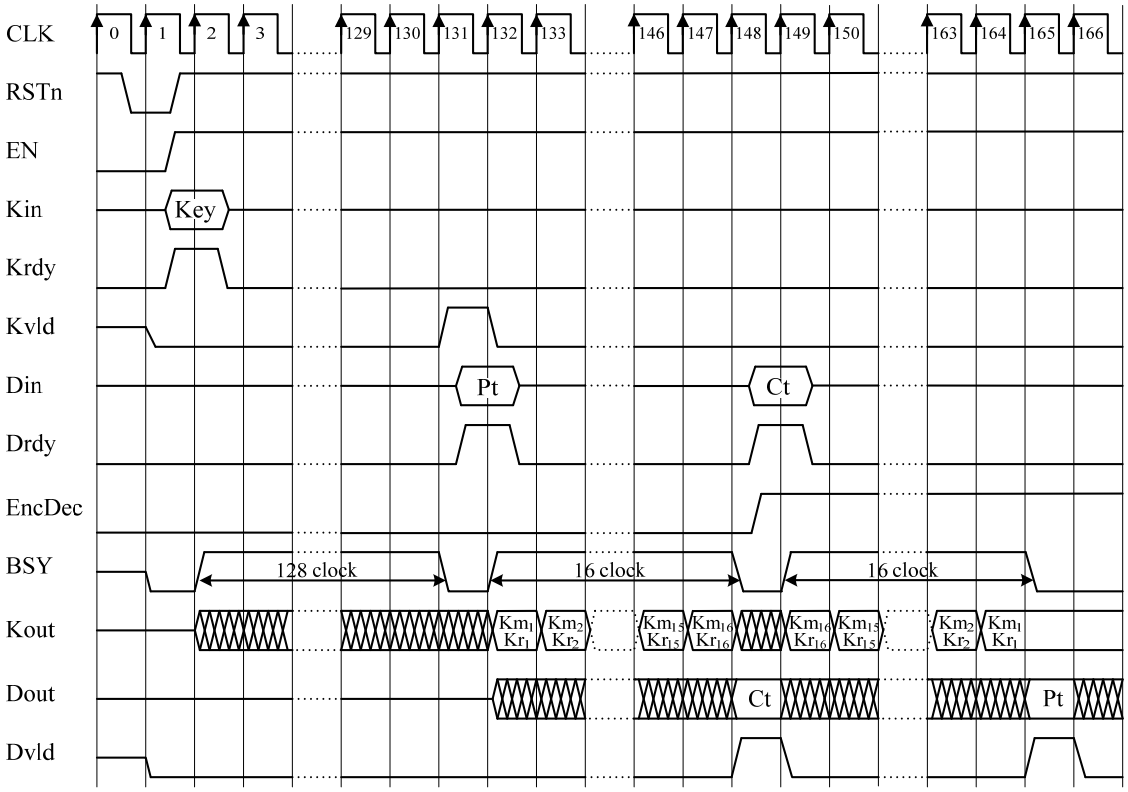


図 5.23 CAST-128 のタイミングチャート

5.13 DES

DES[14]の暗号回路マクロ概要を表 3.16 に, I/O ポートを表 5.17 に示す. DES は Feistel 構造を持つブロック暗号であり, 小型回路化に非常に向いている.

表 5.16 DES の概要

アルゴリズム	DES
データブロック長	64 bit
鍵長	64 bit (鍵 56bit+パリティ 8bit)
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	DES.v
記述言語	Verilog-HDL
トップモジュール名	DES
S-box	テーブル実装
スループット	64 bit / 16 clock
ラウンド鍵生成	On-the-fly

表 5.17 DES の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	64	鍵入力.
Kout	Out	128	48bit のラウンド鍵出力. 上位 80bit は 0 でパディングされる.
Din	In	64	データ入力.
Dout	Out	64	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 64bit の秘密鍵が内部レジスタにラッチされる. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 64bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 DES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵が入力されて内部レジスタにセットされると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

図 5.24 に DES 回路のデータパスアーキテクチャを示す. 32bit のラウンド関数ブロックを 16 回使用する, シンプルな実装を行っている. 64bit 鍵からパリティ 8 ビットを除いた 56 ビット鍵がレジスタ Kreg にセットされるが, このときパリティの検査は行っていない. 鍵スケジュールは on-the-fly で行われ, 暗号化または復号処理中に 48bit のラウンド鍵が 128bit のポート Kout から出力されるが, 上位 80bit は 0 でパディングされる.

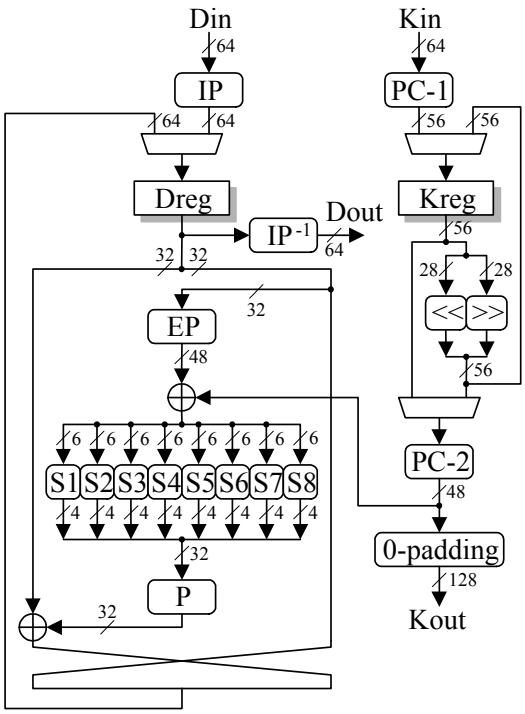


図 5.24　DES のデータパスアーキテクチャ

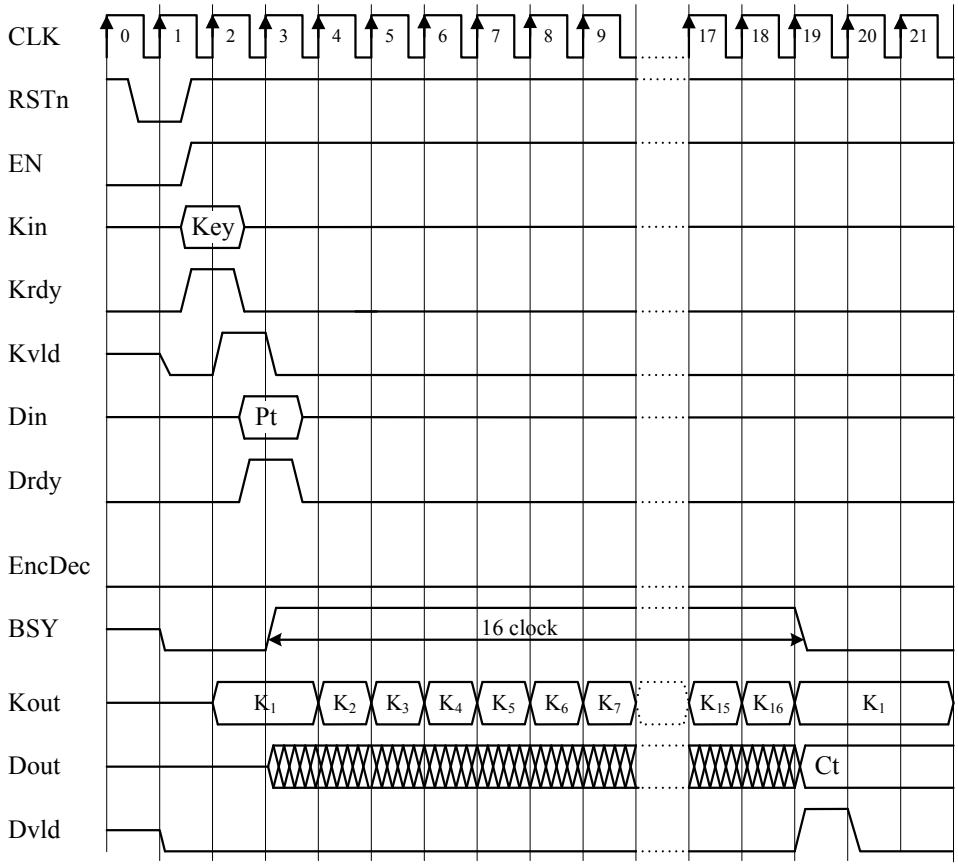


図 5.25　DES のタイミングチャート

図 5.25 に最短サイクルでの暗号化のタイミングチャートを示す. 復号のタイミングチャートはラウンド鍵が K16→K1 の順番で使用される以外は, 暗号化とまったく同じである. 各クロックの動作を下記に示す.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.
CLK2: Krdy=1 とすることで, 64bit ポート Kin に入力された秘密鍵が内部レジスタにセットされる.
CLK3: 事前の鍵スケジュール処理は不要なので, 直ちに鍵が有効になったことを示すフラグ Kvld=1 となる. また EncDec=0(暗号化), そして Drdy=1 とすることで 64bit ポート Din 上の平文がデータレジスタ Dreg にストアされる.
CLK4: 暗号化処理が開始され, BSY=1 となる. Dreg の途中結果が 64bit ポート Dout から出力されるのと同時に, ラウンド鍵 K1 が Kout から出力される. このように暗号化処理の間, 途中結果とラウンド鍵が毎クロック出力される.
CLK20: 暗号化処理が 16 クロックで終了し, BSY=0 となる. 暗号文が Dout から出力されるのと同時に Dvld がこのクロックで 1 となり, 次のクロックですぐに 0 に落ちる.

5.14 ECC

ECCの暗号回路マクロ概要, I/Oポート, そして内部変数に使用する64bit×16wordのメモリマップをそれぞれ, 表5.18~5.20に示す. 本マクロは既約多項式

$$f(x) = x^{61} + x^5 + x^2 + x + 1$$

で定義される有限体GF(2^{61})を用いた楕円曲線

$$E : y^2 + xy = x^3 + ax^2 + b$$

上の点の楕円スカラー倍算処理を行う. 初期点のx座標を61bitデータとして入力するが, データ入力ポートは32bitであるため, x座標61bitの上位に3ビットの0を付加した64bitデータを32bit×2回に分けて入力する. ただし, 鍵である楕円倍算用のスカラー値の入力は64bitであるが, 実際にはMSB 側の 65bit 目が 1 であることを仮定した処理を行っている. つまり, 後述の Algorithm1:Montgomery Powering Ladder 法の中でn-2=65-2=63となっている. なお, 鍵は表5.20のメモリには格納せず, 別途用意した64bitの専用レジスタに格納される.

メモリのアドレス3の64bit(下位61bitが有効)はスカラー乗算の初期点のAffine 座標系におけるx座標を格納する. アドレス4は楕円曲線Eのパラメータbを保持する. アドレス5~7は点の加算と二倍算に用いる中間値を格納する. ただしアドレス5は, MODE=1のときに乱数の格納に用いる. アドレスDと9の変数(X_1, Z_1)は射影座標系で表される初期点を格納し, アドレスEとAの変数(X_2, Z_2)は(X_1, Z_1)を二倍した点を格納する. 射影座標系の入力は, 将来, Z座標にランダムな値(但し0を除く mod $f(x)$による多項式剰余)を用いるサイドチャネル攻撃対策を実装するためである. 現在は対策が未実装のため, 乱数ではなく, Z_1=1としても変わりはない.

なお, 本ECCマクロでは無限遠点のチェック行っていないため, 途中結果が無限遠点となると正しい演算が行われないので, 注意が必要である.

表5.18 ECC回路の概要

アルゴリズム	Montgomery Power Ladder による GF(2^{61})上の楕円スカラー倍算
データブロック長	61 bit (上位 3 ビットは 0 とする)
鍵長	64 bit (スカラー)
機能	GF(2^{61})上の楕円スカラー倍算
ソースファイル名	uec_input_to_ECC_OS.v
記述言語	Verilog-HDL
トップモジュール名	uec_ECC_OS

表 5.19 ECC 回路の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	32	鍵入力. 64bit の鍵(スカラー)と 32bit の乱数(現在のマクロでは未使用)の計 96bit を 3 クロックに分けて入力する.
Din	In	32	上位 3 ビットを 0 でパディングした 64bit のデータとして, affine 座標系の初期点の x 座標, projective 座標系の Z, 曲線パラメータの b をそれぞれ, 2 回に分けて計 6 クロックで入力.
Dout	Out	32	64bit(上位 3 ビットは 0 でパディング)の楕円スカラー倍算結果の x 座標をデータとして, 2 回に分けて出力.
Krdy	In	1	Krdy=1 とした後の 2 クロックで, Kin に入力された 32bit×2 の鍵が内部レジスタにラッチさる.
Drdy	In	1	この信号を 1 クロックだけ Drdy=1 とすることで, 次のクロックから連続する 32bit×6 のデータが内部レジスタにラッチされ, 楕円スカラー倍算処理が開始される.
MODE	In	3	MODE="000"として, べき乗剰余演算アルゴリズムに Montgomery powering ladder 法を指定する. 将来は MODE="001"で, サイドチャネル対策を施した演算を行う予定である.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 ECC マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. 楕円スカラー倍算の計算結果の出力直後およびリセット時に 0, それ以外で 1 となる.
Kvld	Out	1	鍵の入力がが完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐにデータの取り込みが可能となる.
Dvld	Out	1	スカラー倍算処理が完了すると, 1 クロックの間だけ Dvld=1 となり, 次のクロックですぐに 0 に落とされ, また楕円スカラー倍算点の x 座標が Dout から 2 クロックかけて出力される.

表 5.20 ECC 回路のメモリマップ

アドレス	用途	アドレス	用途
0	予約	8	予約
1	予約	9	Z_1
2	予約	A	Z_2
3	x	B	予約
4	b	C	予約
5	t_1 (Rnd)	D	X_1
6	t_2	E	X_2
7	t_3	F	予約

本 ECC 回路では楕円スカラー倍算に，射影座標上の Montgomery Powering Ladder 法 [15]である Lopez と Dahab のアルゴリズム [16]を採用している．また，乗剰余演算は Knezevic らの Montgomery 乗算アルゴリズム [17]を用いている．これらのアルゴリズムをそれぞれ Algorithm 1~3 に示す．

● Algorithm 1： Montgomery Powering Ladder 法

入力：楕円曲線上の点 P, 正の整数 $k=(1k_{n-2}\cdots d_1d_0)_2$

出力：kP の x 座標 kP_x

1: $P_1 \leftarrow P, P_2 \leftarrow 2P$
2: **for** i=n-2 **downto** 0 **do**
3: **if** d_i=1 **then**
4: $x(P_1) \leftarrow x(P_1)+x(P_2),\ x(P_2) \leftarrow x(2P_2)$
5: **else**
6: $x(P_2) \leftarrow x(P_2)+x(P_1),\ x(P_1) \leftarrow x(2P_1)$
7: **end if**
8: **end for**
9: **return** P_{1x}

● Algorithm 2： Lopez と Dahab のアルゴリズム．Montgomery Powering Ladderin Projective Coordinates

入力：$P_1=(X_1,Z_1), P_2=(X_2,Z_2), x=(P_2-P_1)_X$

出力：$P_1=P_1+P_2$

1: $X_1 \leftarrow X_1Z_2$
2: $Z_1 \leftarrow X_2Z_1$
3: $t_1 \leftarrow X_1Z_1$
4: $Z_1 \leftarrow X_1+Z_1$
5: $Z_1 \leftarrow Z_1Z_1$
6: $X_1 \leftarrow xZ_1+t_1$
7: **return** P_1

入力：$P_1=(X_1,Z_1)$

出力：$P_1=2P_1$

1: $t_2 \leftarrow X_1X_1$
2: $t_3 \leftarrow Z_1Z_1$
3: $Z_1 \leftarrow t_2t_3$
4: $t_2 \leftarrow t_2t_2$
5: $t_3 \leftarrow t_3t_3$
6: $X_1 \leftarrow bt_3+t_2$
7: **return** P_1

● Algorithm 3： Knezevic のアルゴリズム．Barrett Reduction over $GF(2^n)$ without precomputation

入力：多項式基底入力 $A(x)=\sum_{i=0}^{2n}a_ix^i$, $M(x)=x^n+\sum_{i=0}^{l}m_ix^i$

ただし，$l=\left\lfloor\frac{n}{2}\right\rfloor$, $a_i, m_i \in \{0,1\}$

出力：$R(x)=A(x) \bmod M(x)$

1: $Q_1(x) \leftarrow A(x) \operatorname{div} x^n$
2: $Q_2(x) \leftarrow M(x)Q_1(x)$
3: $Q_3(x) \leftarrow Q_2(x) \operatorname{div} x^n$
4: $R_1(x) \leftarrow A(x) \bmod x^n$
5: $R_2(x) \leftarrow M(x)Q_3 \bmod x^n$
6: $R(x) \leftarrow R_1(x)+R_2(x)$
7: **return** $R(x)$

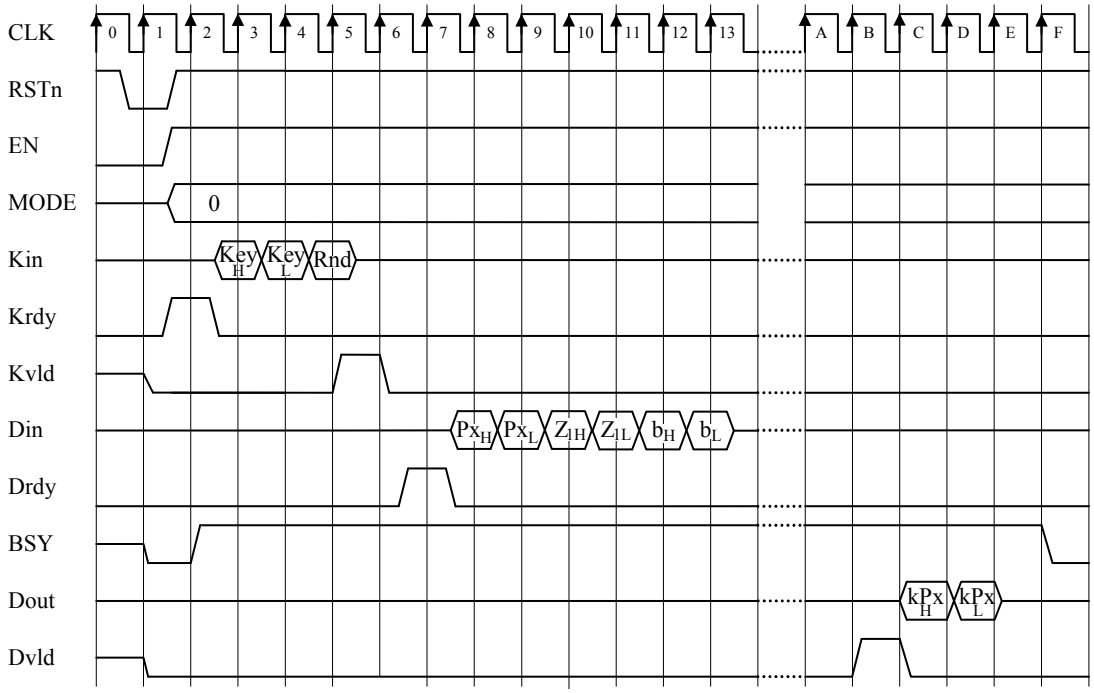


図 5.26 ECC の楕円スカラー倍算処理のタイミングチャート

図 5.26 に本 ECC 回路のタイミングチャートを示す. なお楕円スカラー倍算アルゴリズムは Montgomery Powering Ladder 法(MODE=0)のみ指定可能である. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.
CLK2: EN=1, Krdy=1 とすることで, 次のクロックから, 鍵(スカラー)が取り込まれる.
CLK3: 32bit ポート Kin に入力された鍵 Key の上位 32 ビット Key_H がラッチされる. またビジーフラグ BSY=1 となる.
CLK4: 鍵 Key の下位 32bit Key_L が入力される.
CLK5: サイドチャネル攻撃対策用の乱数 Rnd を入力する. (ただし現在は未サポート)
CLK6: 鍵入力が終了したので Kvld が 1 クロックだけ 1 となる.
CLK7: 次のクロックからデータを取り込むために, Drdy=1 とする.
CLK8~9: affine 座標系における初期点 P の x 座標 P_x の上位 32bit $P_{x\mathrm{H}}$ と下位 32bit $P_{x\mathrm{L}}$ が続けて入力される.
CLK10~13: 射影座標系の Z_1 と曲線パラメータ b が 32bit ずつ 4 クロックで入力される.
CLK14~: 約 7800 クロックを要してスカラー倍算が実行される.
CLKC: 倍算処理が完了し Dvld=1 となったので, 次のクロックから結果が出力される.
CLKD: 楕円スカラーk 倍算(k は鍵 Key の値)結果の点 kP の x 座標の上位 32bit の $kP_{x\mathrm{H}}$ が出力される.
CLKE: kP の x 座標の下位 32bit の kP_{xL} が出力される.

5.15 MISTY1

MSITY1[18]の暗号回路マクロ概要を表 5.21 に, I/O ポートを表 5.22 に示す. MSITY1 は入れ子型の Feistel 構造を持つブロック暗号である.

表 5.21 MISTY1 の概要

アルゴリズム	MISTY1
データブロック長	64 bit
鍵長	128 bit
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	MISTY1_1clk.v
記述言語	Verilog-HDL
トップモジュール名	MISTY1
S-box	テーブル実装
スループット	64 bit / 9 clock
ラウンド鍵生成	On-the-fly

表 5.22 MISTY1 の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	256	128bit の秘密鍵に 128bit の中間鍵が連節されて出力される.
Din	In	64	データ入力.
Dout	Out	64	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 128bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 MISTY1 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

図 5.27 に MISTY1 回路のデータパスアーキテクチャを示す. 1 ラウンドは 1 クロックで実行され, 64bit のデータブロックの暗号化または復号処理は 9 クロックで完了する. 128bit の秘密鍵がポート Kin から入力されると, 直ちに 8 クロックかけて中間鍵の生成がデータランダム化部で行われる. その後に, 平文または暗号文データを 64bit ポート Din に入力することで, 暗号化または復号が開始され, 対応する暗号文または平文が 64bit ポート Dout から出力される.

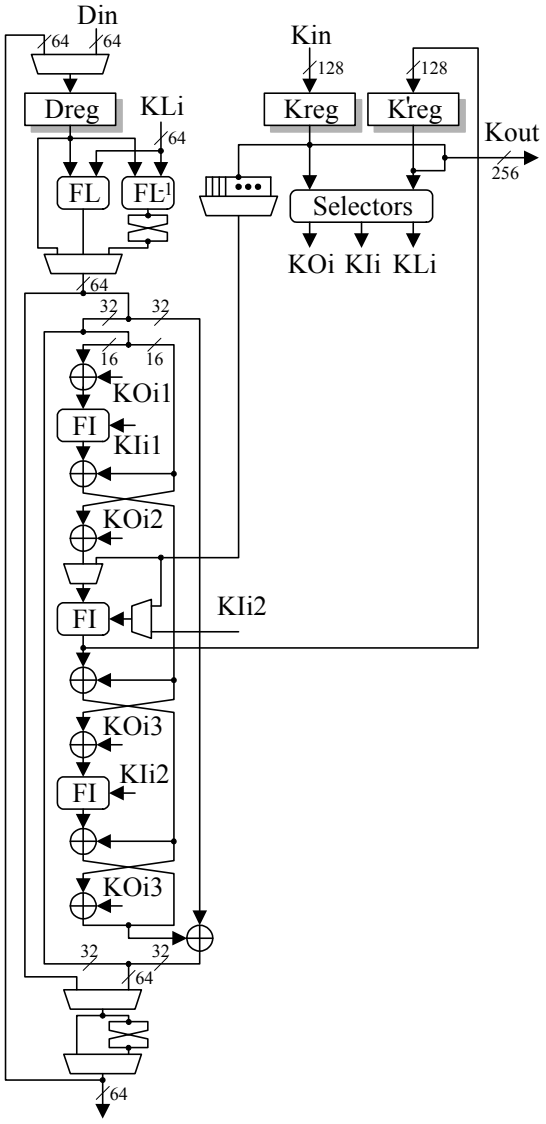


図 5.27 MISTY1 のデータパスアーキテクチャ

図 5.28 に MISTY1 回路の最短サイクルでの鍵スケジュール, 暗号化, 復号のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.

CLK2: Krdy=1 とすることで, Kin に入力された 128bit の秘密鍵が内部レジスタ Kreg にセットされる.

CLK3: 中間鍵生成の鍵生成処理が開始され, ビジー信号 BSY=1 となる.

CLK10: 中間鍵の生成が終了しレジスタ K'reg にセットされ, BSY=0, また 1 クロックだけ Kvld=1 となる.

CLK11: Drdy=1 とすることで, Din に入力された 64bit の平文 PT が内部レジスタ Dreg にセットされ

る.

CLK12: EncDec＝0 なので暗号化処理が開始され, ビジー信号 BSY=1 となる. これから毎クロック, Dout に途中結果が, Kout にラウンド鍵が出力されていく.

CLK13~20: 暗号化処理が 9 クロックで完了し, 64bit の暗号文 CT が Dout から出力され, BSY=0, データ出力信号 Dvld が 1 クロックだけ 1 となる.

CLK21: EencDec=1, Drdy=1 とすることで, Din に入力された 64bit の暗号文 CT が内部レジスタ Dreg にセットされる.

CLK22: EncDec＝1 なので復号処理が開始され, ビジー信号 BSY=1 となる. これから毎クロック, Dout に途中結果が, Kout にラウンド鍵が出力されていく.

CLK23~30: 復号処理が 9 クロックで完了し, 64bit の平文 PT が Dout から出力され, BSY=0, データ出力信号 Dvld が 1 クロックだけ 1 となる.

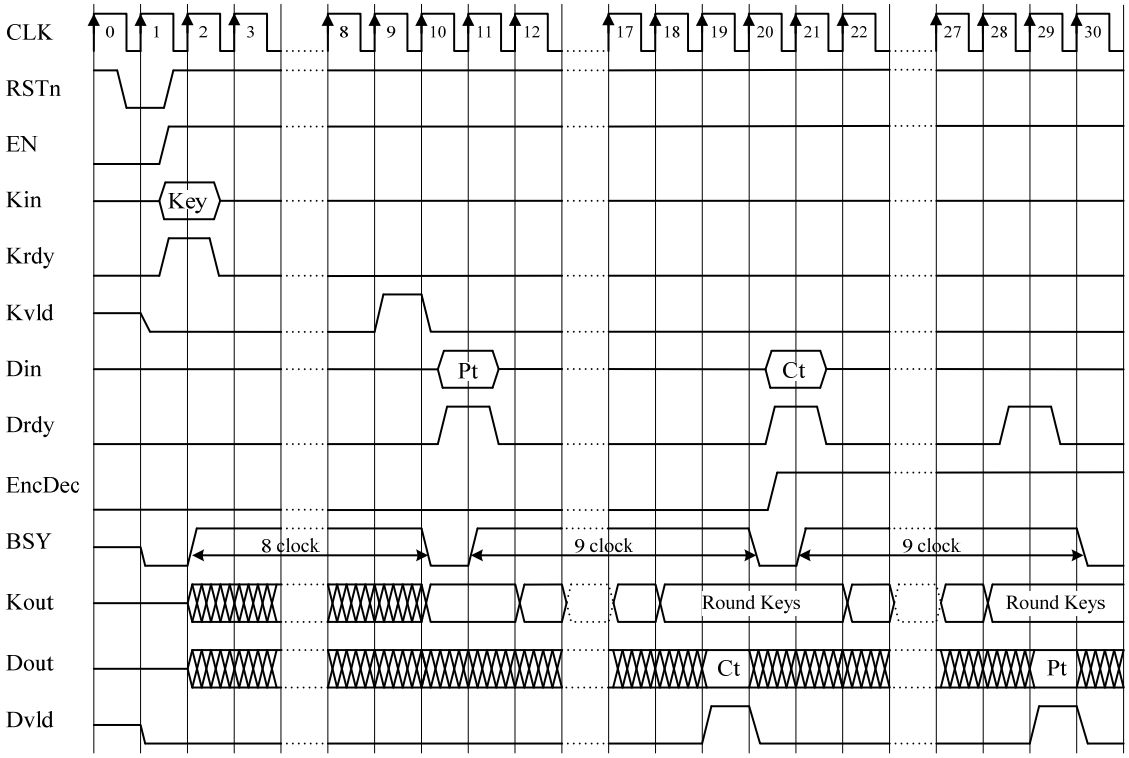


図 5.28 MISTY1 のタイミングチャート

5.16 RSA

RSA の暗号回路マクロ概要を表 5.23 に, I/O ポートを表 5.24 に示す. 本マクロは, RSA 暗号 [19] の 512bit 暗号化および復号を, 6 種類のべき乗剰余演算アルゴリズムによって実行することができる. バイナリ法(左バイナリ法および右バイナリ法 [20])による基本的な実装に加え, サイドチャネル攻撃への対策として square-and-multiply always method(ダミー演算による対策法)[21], Montgomery Powering Ladder[22], そして Square-Multiply べき乗法 [23], が実装されている. さらに, Chinese Remainder Theorem (CRT) [24]による高速実装にも対応しており, べき乗算剰余演算と組み合わせることで計 12 種類から演算手法を選択することができる. 乗剰余演算には Finely Integrated Operand Scanning (FIOS) [25]の高基数モンゴメリ乗算アルゴリズムを用いている.

表 5.23 RSA の概要

アルゴリズム	RSA
データブロック長	512 bits
鍵長	512 bits
機能	CRT モード(non-CRT/CRT) べき乗剰余演算 0)左バイナリ法 1) 右バイナリ法 2) 左バイナリ法+ダミー乗算 [21)] 3) 右バイナリ法+ダミー乗算 [21)] 4) Montgomery Powering Ladder[22)] 5) Square-Multiply べき乗法 [23)]
ソースファイル名	RSA.v
記述言語	Verilog-HDL
トップモジュール名	RSA
スループット	non-CRT 512 bit / 約 452K clocks – 0) 1) 512 bit / 約 599K clocks – 2) 3) 4) 5) CRT 512 bit / 約 135K clocks – 0) 1) 512 bit / 約 176K clocks – 2) 3) 4) 5)

表 5.24 RSA の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	32	鍵入力. 512 ビットの鍵データを最下位ビットから 32 ビット毎, 16 サイクルかけてシーケンシャルに入力. CRT 適用時には, 2 つの鍵, それぞれ 256 ビットを 32 ビット毎に 8 クロックずつ続けて入力する.
Min	In	32	法入力. 512 ビットの法データ N (=pq)を最下位ビットから 32 ビット毎に 16 クロックかけてシーケンシャルに入力. CRT 適用時には, 2 つの法, それぞれ 256 ビットを 32 ビット毎に 8 サイクルずつ続けて入力する. さらにその後続けて, 前処理演算の値 $U=q^{-1} \bmod p$ を 8 クロックかけて入力する.
Din	In	32	データ入力. 512 ビットのデータを最下位ビットから 32 ビット毎, 16 クロックかけてシーケンシャルに入力する.
Dout	Out	32	データ出力. Dvld=1 が出力された後, 512 ビットのデータを最下位ビットから 32 ビット毎, 16 クロックかけてシーケンシャルに出力する.
Krdy	In	1	Krdy=1 とした後, 内部のレジスタに鍵を取り込む. Mrdy と Krdy の両方が 1 のときは, Krdy を優先する.
Mrdy	In	1	Mrdy=1 とした後, 法への入力を内部のメモリに取り込む.
Drdy	In	1	Drdy=1 とした後, データへの入力を内部のメモリに取り込む. その後, 続けて暗号化を開始する.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.

EN	In	1	イネーブル信号. EN=1 のとき, 本 RSA 暗号マクロがアクティブとなる.
CRT	In	1	CRT=1 の時に CRT 処理が適用される(CRT). CRT=0 の時には, CRT 処理は適用されない(non-CRT).
MODE	In	3	べき乗剰余演算の動作モードを指定する. MODE=0, 1, 2, 3, 4, 5 の時に, それぞれ 0)左バイナリ法, 1)右バイナリ法, 2)ダミー乗算付き左バイナリ法, 3) ダミー乗算付き右バイナリ法, 4)Montgomery Powering Ladder, 5)square-multiply べき乗法が適用される.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	処理中であることを表すフラグ. 暗号化, もしくはデータを取り込んでいる時に 1 となる. この間, Drdy, Mrdy, Krdy の変化は無視される.
Kvld	Out	1	512bit 鍵が取り込まれると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 に落とされる.
Mvld	Out	1	法が取り込まれると, 1 クロックの間だけ Mvld=1 となり, 次のクロックですぐに 0 に落とされる.
Dvld	Out	1	べき乗剰余演算の処理が完了すると, 1 クロックの間だけ Dvld=1 となり, 次のクロックですぐに 0 に落とされる.

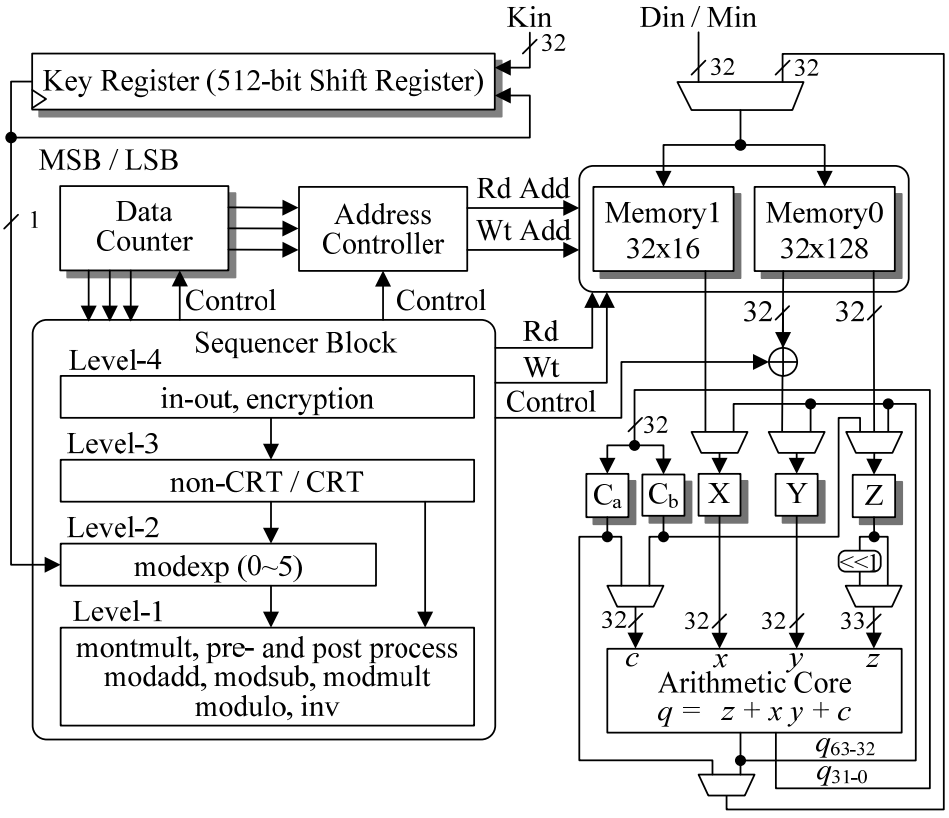


図 5.29　RSA 暗号マクロの回路アーキテクチャ

図 5.29 に RSA 暗号マクロの回路アーキテクチャを示す. 本マクロは, 鍵レジスタ(Key Register), 制御ブロック(Sequencer Block), 演算ブロック(Multiplication Block), カウンタモジュール(Data Counter), メモリ(Memories), アドレスコントローラ(Address Controller)からなる. 鍵レジスタは, 512 ビットの鍵を格納するシフトレジスタで, べき乗剰余演算のシーケンスに従い 1 ビットずつシーケンシャルに鍵情報を制御ブロックへと出力する. カウンタは, 値を保持する 3 つのレジスタ(9 ビットレジスタ 2 つと 4 ビットレジスタ 1 つ)と 9 ビットの加算器からなる. メモリは 2 つのレジスタアレイを有する. アドレスコントローラは, レジスタアレイのためのアドレスを生成する.

制御ブロックは Level-1~4 の 4 階層から構成され, まず, Level-4 は入出力制御を行う. Level-3 では CRT モードを, Level-2 では, 6 種類のべき乗剰余演算のシーケンスを, Level-1 ではべき乗剰余演算および CRT に必要な各関数の演算シーケンスをそれぞれ制御する. 具体的な演算としては, Montgomery 乗算(montmult), Montgomery 乗算の前処理演算(montredc, inv), 多倍長剰余演算各種(剰余算(modulo), 剰余加算(modadd), 剰余減算(modsub)), 多倍長乗算(mult)およびデータ移動およびコピー等の制御をサポートしている.

図 5.30 に RSA 回路マクロの, CRT 処理を行わない non-CRT(CRT=0)の場合のタイミングチャートを示す. また, べき乗剰余演算アルゴリズムとして左バイナリ法 modexp0(MODE=0)を指定している. なお, 入力信号は全て最短のタイミングで制御している. 右バイナリ法および対策版アルゴリズムを使用した場合にも, 同様のタイミングチャートとなる. しかしながら暗号化のサイクル数は異なり, 右バイナリ法ではおよそ 452K サイクル, 対策アルゴリズムではそれぞれおよそ 599K サイクルである.

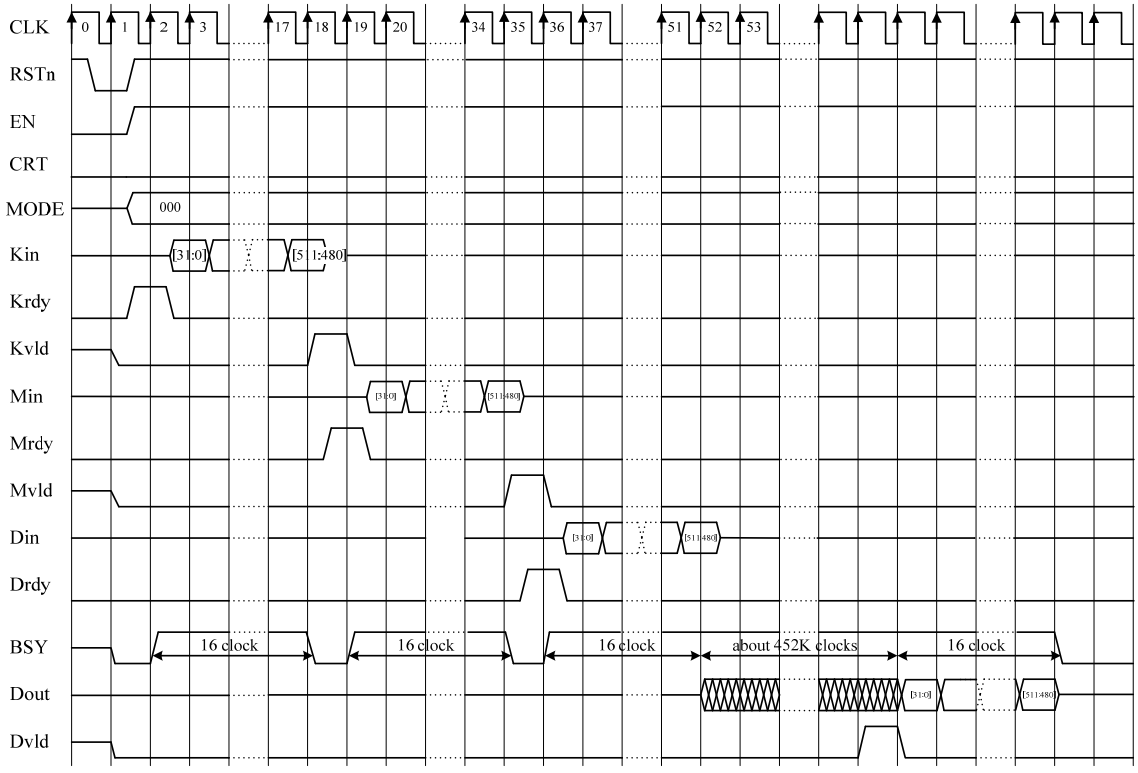


図 5.30　RSA のタイミングチャート(non-CRT)

CLK1: RSTn=0 とすることで, シーケンサおよびレジスタをリセットする.

CLK2: EN=1, CRT=0, MODE=000 とする.

CLK2~18: Krdy=1 とした後, 鍵データ 512 ビットを内部の鍵レジスタに格納する. 入力ポートが 32 ビットであるため, 最下位ビットから 32 ビット毎にシーケンシャルに入力する. この時 BSY=1 となる. その 16 クロック後に BSY=0 となり, アイドリング状態となる. また, CLK18 に Kvld=1 が 1 クロックの間出力される.

CLK19~35: Mrdy=1 とした後，法データ 512 ビットをメモリに格納する．鍵データ同様，最下位ビットから 32 ビット毎にシーケンシャルに入力する．このとき BSY=1 となる．その 16 クロック後に BSY=0 となり，アイドリング状態に移行する．また，CLK35 に Mvld=1 が 1 クロックの間出力される．

CLK36~52: 鍵および法が格納された状態で Drdy=1 とすると，平文データ 512 ビットがメモリに格納される．平文データは最下位ビットから 32 ビット毎にシーケンシャルに入力する．BSY=1 となり，平文入力が終了すると，そのまま暗号化状態に移行する．

CLK53~: およそ 452K クロックかけてべき乗剰余演算が実行される．処理終了後，Dvld=1 が 1 クロックの間だけ出力される．その後 16 クロックをかけて，暗号文データを最下位ビットから 32 ビット毎にシーケンシャルに演算結果として出力すると，BSY=0 となり，アイドリング状態に移行する．

図 5.31 に CRT 演算を適用した場合のタイミングチャートを示す．法および鍵の入力法が異なり，また暗号化状態のサイクル数が異なること以外は，図 5.30 とほぼ同じとなる．CRT 演算では，2 つの法および鍵が必要になるため，CLK2~18 および CLK19~35 において鍵と法が 2 つずつ，それぞれ 256 ビットを 32 ビット毎に 8 サイクルずつ入力される．さらに CLK36~43 には，法入力に続き前処理の演算($U= q^{-1} \bmod p$ ここで $N=pq$)の値が 8 サイクルかけて入力される．つまり，Mrdy=1 に伴う入力操作は 24 サイクルとなる．CRT 演算を適用することでサイクル数は，バイナリ法および対策アルゴリズムでそれぞれおよそ 135K および 176K サイクルとなる．

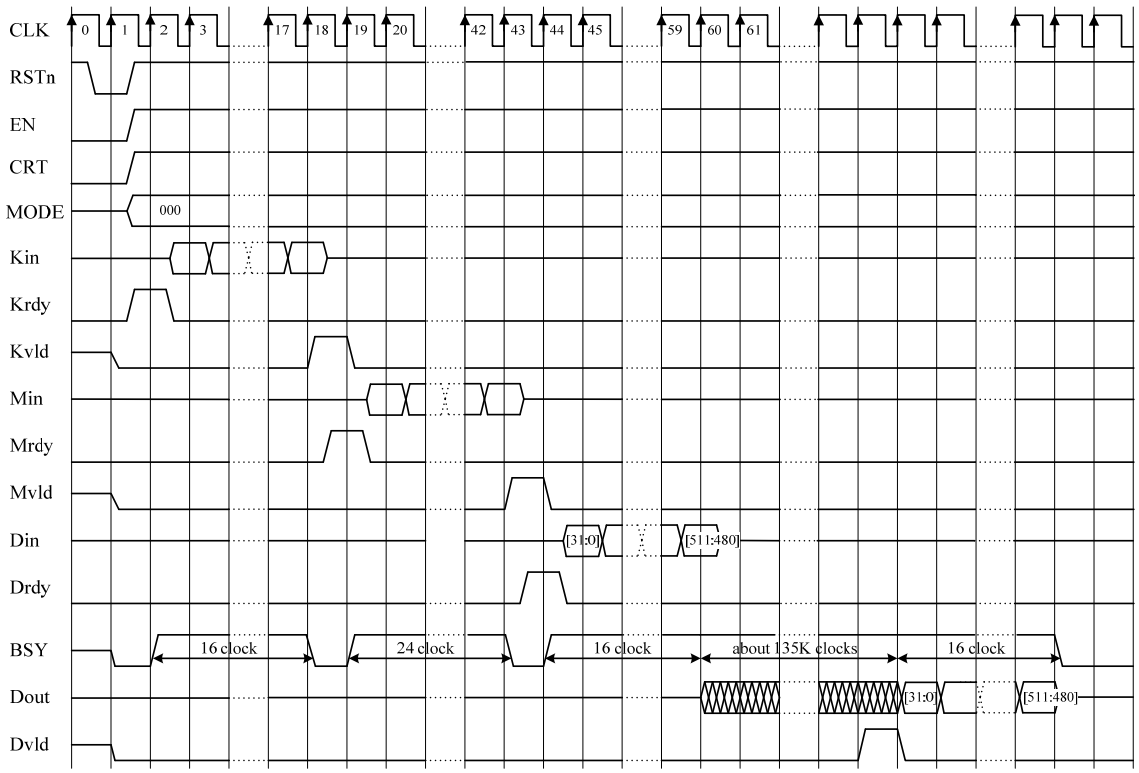


図 5.31 RSA のタイミングチャート(CRT)

5.17 SEED

SEED[26]の暗号回路マクロ概要を表 5.25 に，I/O ポートを表 5.26 に示す．SEED は KISA (Korea Information Security Agency)によって提案された Feistel 構造を持つブロック暗号である．

表 5.25 SEED の概要

アルゴリズム	SEED
データブロック長	128 bits
鍵長	128 bits
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	SEED.v
記述言語	Verilog-HDL
トップモジュール名	SEED
S-box	テーブル実装
スループット	128 bit / 23 clock
ラウンド鍵生成	事前計算 & On-the-fly

表 5.26 SEED の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	128	鍵入力.
Kout	Out	128	ラウンド鍵出力.
Din	In	128	データ入力.
Dout	Out	128	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に入力された 128bit の秘密鍵が内部レジスタにラッチされ, 鍵の初期化処理が開始される. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 128bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	鍵初期化処理が完了すると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

SEED のデータパスアーキテクチャを図 5.32 に示す. 1 ラウンドは 1 クロックで処理され, 128bit の平文または暗号文を暗号化または復号するのに, いずれも 16 クロックを要する. 64bit のラウンド関数は, 32bit の G 関数と XOR そして加算(または減算)のセットを 3 回使う MISTY1 と類似のいれこ型の構造をしている. G 関数は 4 つの 8bit S-boxes と 32bit の Permutation 関数から構成される. 64bit の 16 個のラウンド鍵 K1~K16 は 128bit の秘密鍵を巡回シフトした後に, 加減算と G 関数によって on-the-fly で生成される.

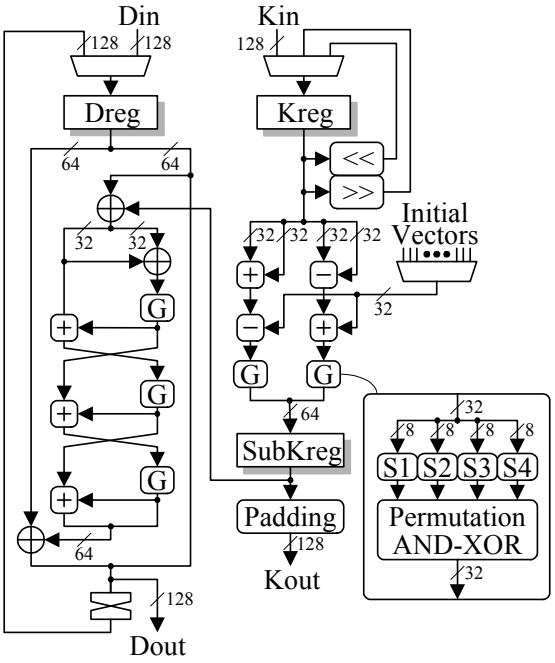


図 5.32 SEED のデータパスアーキテクチャ

図 5.33 に最短サイクルでの鍵スケジュール, 暗号化, 復号のタイミングチャートを示す. 各クロックの動作は下記の通りである.

CLK1: RSTn=0 とすることで, 制御回路がリセットされる.

CLK2: EncDec=0, Krdy=1 とすることで, 暗号化のために 128bit ポート Kin に入力された秘密鍵 Key が内部レジスタにセットされる.

CLK3:鍵スケジュール処理が開始され, ビジーフラグ BSY=1 となる. この処理はこのクロックで完了しており, 同時に 1 クロックだけ Kvld=1 となる. EncDec の値を変えて, 暗号化から復号に移る時にも鍵スケジュールを再実行する必要がある. この段階で, 暗号化の最初のラウンド鍵 K_1 が 128bit ポート Kout に出力されている.

CLK4: Drdy=1 とすることで 128bit ポート Din 上の平文 Pt がデータレジスタ Dreg にストアされる. 鍵スケジュールが終了したので BSY=0 となる.

CLK5: 暗号化処理が開始され, BSY=1 となる. Dreg の途中結果が 128bit ポート Dout から出力されるのと同時に, ラウンド鍵 K_2 が Kout から出力される. これ以降も, 途中結果とラウンド鍵が毎クロック出力される.

CLK20: 暗号化処理が 16 クロックで終了し, BSY=0 となる. 暗号文 Ct が Dout から出力されるのと同時に Dvld がこのクロックで 1 となり, 次のクロックですぐに 0 に落ちる.

CLK21: EncDec=1, Krdy=1 とすることで, 復号用の秘密鍵 Key が内部レジスタにセットされる.

CLK22: 鍵スケジュール処理が開始され, ビジーフラグ BSY=1 となる. この処理はこのクロックで完了しており, 同時に 1 クロックだけ Kvld=1 となる. この時, 復号の最初のラウンド鍵 K_{16} がポート Kout に出力されている

CLK23: Drdy=1 とすることで 128bit ポート Din 上の暗号文 Ct がデータレジスタ Dreg にストアされる. 鍵スケジュールが終了したので BSY=0 となる.

CLK24: 復号処理が開始され BSY=1 となる. 暗号化と同様に途中結果とラウンド鍵が毎クロック Dout と Kout から出力される.

CLK39: 復号が 16 クロックで完了し BSY=0 となる. 平文 Pt が Dout から出力され, Dvld がこのクロックだけ 1 となる.

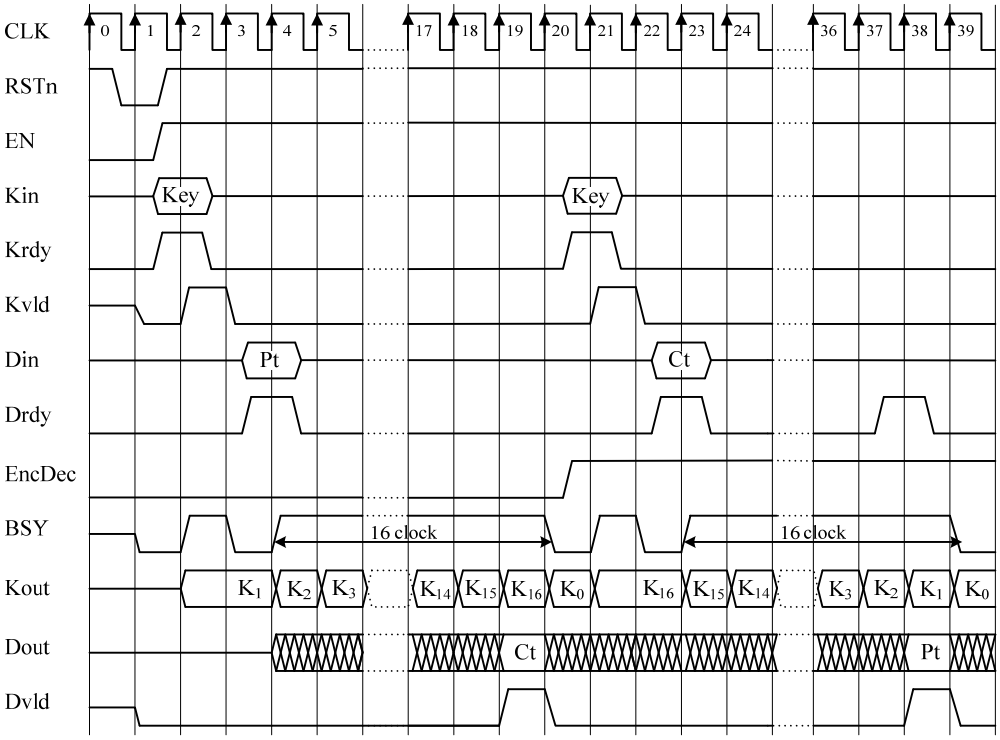


図 5.33 SEED のタイミングチャート

5.18 TDES

TDES (Triple-DES)[14]の暗号回路マクロ概要を表 5.27 に, I/O ポートを表 5.28 に示す. TDES は 56bit 鍵の DES の処理を, 鍵を変えながら TDES 暗号化では「DES 暗号化-DES 復号-DES 暗号化」, TDES 復号では「DES 復号-DES 暗号化-DES 復号」と 3 回(16 サイクル×3 回=48 サイクル)繰り返すものである. 本マクロでは, 3 つの異なる鍵を用いる 3-key Triple-DES をサポートしている. 3 つの鍵を連続して 3 クロックでセットするが, このとき最初と最後の鍵を同じにすると 2-key Triple-DES となる. また 3 つの鍵を全て同じにすると, DES 暗号化と DES 復号が相殺されるので, 単純な DES の処理と等価となる(ただしサイクル数は 3 倍の 48 クロックのままである).

表 5.27 TDES の概要

アルゴリズム	3-key Triple-DES
データブロック長	64 bit
鍵長	64 bit (鍵 56bit+パリティ 8bit)×3
機能	暗号化/復号
暗号利用モード	Electronic Code Book (ECB)
ソースファイル名	TDEA.v
記述言語	Verilog-HDL
トップモジュール名	TDEA
S-box	テーブル実装
スループット	64 bit / 48 clock
ラウンド鍵生成	On-the-fly

表 5.28 TDES の I/O ポート

ポート名	方向	ビット幅	説明
Kin	In	64	鍵入力.
Kout	Out	128	48bit のラウンド鍵出力. 上位 80bit は 0 でパディングされる.
Din	In	64	データ入力.
Dout	Out	64	データ出力.
Krdy	In	1	この信号が Krdy=1 のとき, Kin に 3 クロックを要して入力された 64bit×3 個の秘密鍵が順次内部レジスタにラッチされる. もし Drdy と Krdy に同時に '1' が入力された場合は, Krdy が優先される.
Drdy	In	1	この信号が Drdy=1 のとき, Din に入力された 64bit の平文(または暗号文)データが 内部レジスタにラッチされ, 暗号化(または復号)処理が開始される.
EncDec	In	1	Drdy=1 のときに, EncDec=0 ならば暗号化処理が, EncDec=1 ならば復号処理が行われる.
RSTn	In	1	リセット信号. このポートに 0 が入力されると, 制御回路と内部レジスタがリセットされる. リセット処理はイネーブル信号が EN=0 でも, システムクロック CLK が入力されている限りいつでも実行することができる.
EN	In	1	イネーブル信号. EN=1 のとき, 本 TDES 暗号マクロがアクティブとなる.
CLK	In	1	システムクロック. すべての内部レジスタは, このクロックの立ち上がりエッジに同期してデータを取り込む.
BSY	Out	1	ビジーステータスフラグ. このフラグは, 暗号化/復号/鍵初期化処理が行われている間, 1 にセットされる. BSY=1 の間は Drdy および Krdy 信号は無視される.
Kvld	Out	1	3 つの鍵が順次入力され, 3 つの内部レジスタにセットされると, 1 クロックの間だけ Kvld=1 となり, 次のクロックですぐに 0 の落とされる. この後すぐに暗号化および復号処理が実行可能となる.
Dvld	Out	1	暗号化(または復号)処理が完了し, 暗号文(または平文)がデータ出力ポート Dout にセットされると, 1 クロックの間だけ Dryd=1 となり, 次のクロックですぐに 0 に落とされる.

図 5.34 に TDES 回路のデータパスアーキテクチャを示す. DES 回路との違いは鍵レジスタが 3 個になっただけであり, ラウンド処理は DES と同様一つの 32bit 関数ブロックが用意されており, それを 48 回繰り返し使用する, シンプルな実装である. 64bit 鍵からパリティ 8bit を除いた 56bit 鍵がレジスタ Kreg1~3 にセットされるが, このとき DES 回路と同様にパリティの検査は行っていない. 鍵スケジュールは on-the-fly で行われ, 暗号化または復号処理中に 48bit のラウンド鍵が 128bit のポート Kout から出力されるが, 上位 80bit は 0 でパディングされる.

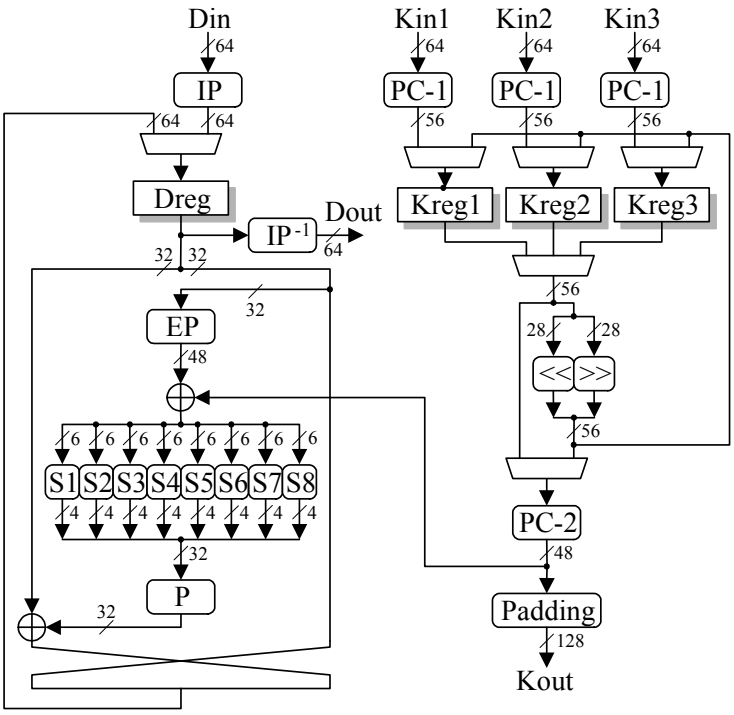


図 5.34 TDES のデータパスアーキテクチャ

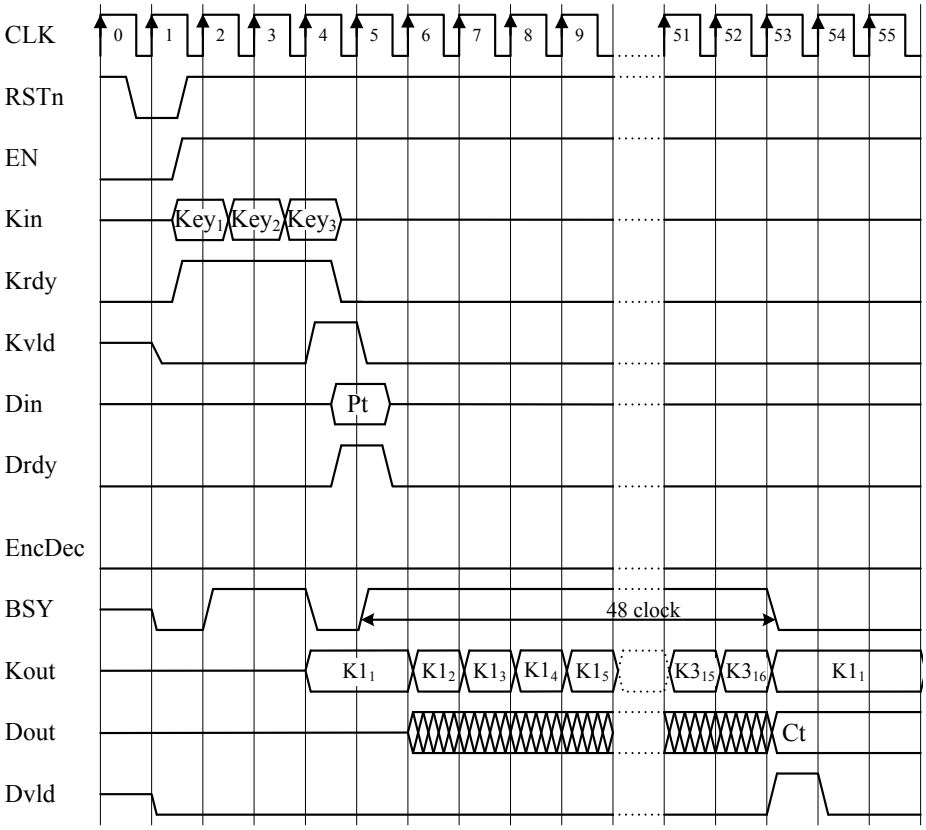


図 5.35 TDES のタイミングチャート

図 5.35 に最短サイクルでの暗号化のタイミングチャートを示す．復号のタイミングチャートはラウンド鍵が K16→K1 の順番で使用される以外は，暗号化とまったく同じである．各クロックの動作は下記に示す．

CLK1: RSTn=0 とすることで，制御回路がリセットされる．

CLK2~4: Krdy=1 とし，64bit ポート Kin に 3 つの秘密鍵 Key_1~Key_3 を順次入力することで，3 つの内部レジスタ Kreg1~3 にセットされる．

CLK5: 事前の鍵スケジュール処理は不要なので，直ちに鍵が有効になったことを示すフラグ Kvld=1 となる．また EncDec=0(暗号化)，そして Drdy=1 とすることで 64bit ポート Din 上の平文 Pt がデータレジスタ Dreg にストアされる．

CLK6: 暗号化処理が開始され，BSY=1 となる．Dreg の途中結果が 64bit ポート Dout から出力されるのと同時に，最初の秘密鍵 Key_1 に対応するラウンド鍵 $K1_1$ が Kout から出力される．このように暗号化処理の間，途中結果とラウンド鍵が毎クロック出力される．

CLK54: 暗号化処理が 48 クロックで終了し，BSY=0 となる．暗号文 Ct が Dout から出力されるのと同時に Dvld がこのクロックで 1 となり，次のクロックですぐに 0 に落ちる．

文献

1) ISO/IEC 18033-3 “Information technology – Security techniques – Encryption algorithm – Part 3: Block ciphers,” Jul. 2005. http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=37972
2) National Institute of Standards and Technology, “FIPS PUB 197: ADVANCED ENCRYPTION STANDARD (AES),” Nov. 2001.
3) A. Satoh, S. Morioka, K. Takano, S. Munetoh, “A Compact Rijndael Hardware Architecture with S-Box Optimization,” Advances in Cryptotology (*ASIACRYPT 2001*), LNCS 2248, pp. 239-254, Springer-Verlag, Dec. 2001.
4) S. Morioka, A. Satoh, “An Optimized S-Box Circuit Architecture for Low Power AES Design,” Workshop on Cryptographic Hardware and Embedded Systems (*CHES 2002*), LNCS 2523, pp. 271-295, Springer-Verlag, Aug. 2002.
5) NIST, “Recommendation for Block Cipher Modes of Operation: Methods and Techniques,” Special Publication 800-38A, Dec. 2001. http://csrc.nist.gov/CryptoToolkit/modes/800-38_ Series_Publications/SP800-38A.pdf
6) E. Trichina, “Combinational Logic Design for AES SubByte Transformation On masked Data,” Cryptology ePrint Archive, 2003/236, 2003.
7) S. Nikova and C. Rechberger, and V. Rijmen, “Threshold Implementations Against Side-Channel Attacks and Glitches,” The 8th International Conference on Information and Communications Security (ICICS 2006), LNCS4307, pp. 529-545, Springer-Verlag, Dec. 2006.
8) T. Pop and S. Mangard, “Masked Dual-Rail Pre-charge Logic: DPA-Resistance without Routing Constrain,” Workshop on Cryptographic Hardwar and Embedded Systems (*CHES2005*), LNCS 3659, pp. 172-186, Springer-Verlag, Aug. 2005.
9) K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” Proc. 2004 Design, Automation and Test in Europe Conference and Exposition (*DATE 2004*), pp. 246-251, Feb. 2004.
10) D. Suzuki, M. Saeki, and T. Ichikawa, “Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E90-A, no. 1, pp. 160-168, Jan. 2007.
11) K.Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, “Specification of Camellia – a 128-bit Block Cipher,” Sep. 2001. http://info.isl.ntt.co.jp/crypt/camellia/dl/01espec.pdf
12) C. Adams, “The CAST-128 Encryption Algorithm,” RFC2144 (Informational), May 1997.
13) T. Sugawara, N. Homma, T. Aoki, and A. Satoh, “A High-Performance ASIC Implementation of the 64-bit Block Cipher CAST-128,” Proc. 2007 IEEE International Symposium on

Circuits and Systems (*ISCAS2007*), pp. 1859-1862, May 2007.

14) NIST, “FIPS PUB 46-3: DATA ENCRYPTION STANDARD (DES),” Oct. 1999.
15) P. L. Montgomery, “Speeding the Pollard and elliptic curve methods of factorization,” Mathematics of Computation, vol. 48, no.177, pp. 243-264, 1987.
16) J. L´opez, and R. Dahab, “Fast multiplication on elliptic curves over $GF(2^m)$,” Workshop on Cryptographic Hardware and Embedded Systems (*CHES ’99*), LNCS 1717, pp. 316-327, Springer-Verlag, Aug. 1999.
17) M. Kne.zevi´c, K. Sakiyama, J. Fan, I. Verbauwhede, “Modular Multiplication in $GF(2^n)$ without Pre-computational Phase,” Proc. WAIFI’08, LNCS 5130, Springer-Verlag, pp. 77-87, 2008.
18) M. Matsui, “Specification of MISTY1 - a 64-bit Block Cipher,” NESSIE Project. https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html
19) R. L. Rivest, A. Shamir, and L. Adliman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
20) J. A. Menezes, C. P. Oorschot, and A. S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997.
21) J. S. Coron: “Resistance against differential power analysis for elliptic curve cryptosystems”, Workshop on Cryptographic Hardware and Embedded Systems (*CHES ’99*), LNCS 1717, pp. 192-302, Springer-Verlag, Aug. 1999.
22) M. Joye and S. M. Yen, “The Montgomery powering ladder”, Workshop on Cryptographic Hardware and Embedded Systems (*CHES2002*), LNCS 2523, pp. 291-302, Springer-Verlag, 2003.
23) M. Joye, “Highly Regular Right-to-Left Algorithms for Scalar Multiplication”, Workshop on Cryptographic Hardware and Embedded Systems (*CHES2007*), LNCS 4727, pp. 135-147, Springer-Verlag, Sep. 2007.
24) J. J. Quisquater and C. Couvreur, “Fast decipherment algorithm for RSA public-key cryptosystem,” *Electronics Letters*, vol. 18, no. 21, pp. 905-907, Oct. 1982.
25) C.K. Koc, T. Acar, and J. Burton S. Kaliski, “Analyzing and comparing Montgomery multiplication algorithms,” IEEE Micro, vol. 16, no. 3, pp. 26-33, Jun 1996.
26) “SEED Algorithm Specification” http://www.kisa.or.kr/seed/data/Document_pdf/SEED_Specification_english.pdf

本暗号 LSI は経済産業省の委託事業において(独)産業技術総合研究所によって開発されました.

This Cryptographic LSI was developed by AIST undertaking projects sponsored by METI (Ministry of Economy, Trade and Industry, Japan)

【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

〒101-0021
東京都千代田区外神田 1-18-13 秋葉原ダイビル 10 階 1003 号室
TEL：03-5298-4722
FAX：03-5298-4522