# 標準暗号 LSI 仕様書
# ~サイドチャネル攻撃対策版(65nm)~

# Standard Cryptographic LSI Specification
## ~ with Side Channel Attack Counter Measures (65nm) ~

**[第 0.9 版]**


**2010 年 8 月 27 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 ..... 3**

**2. 外部仕様 ..... 4**

2.1. 入出力信号 ..... 4
2.2. ピンアサイン ..... 4
2.3. 入出力タイミング ..... 9
2.4. インタフェースレジスタ ..... 11
2.5. 動作手順 ..... 13

**3. 詳細仕様 ..... 15**

3.1. 全体ブロック図 ..... 15
3.2. 階層構造 ..... 15
3.3. 外部インタフェース回路 ..... 17
3.4. 暗号アルゴリズムコアインタフェース ..... 18
3.5. インタフェースレジスタ詳細 ..... 21
3.6. クロックツリー ..... 30
3.7. リセット ..... 31
3.8. 付帯機能および留意事項 ..... 32

**4. 論理シミュレーションによる動作検証用環境 ..... 38**

4.1. 動作検証用モジュール概要 ..... 38
4.2. 動作検証モジュールの機能 ..... 38
4.3. 動作検証モジュールを用いた検証および検証結果 ..... 38

**5. 論理合成制約について ..... 41**

**6. LSI の物理レイアウト ..... 42**

6.1. 設計環境 ..... 42
6.2. 論理合成結果 ..... 42
6.3. 電源プラン ..... 44
6.4. マクロ配置 ..... 47
6.5. モジュール配置 ..... 48
6.6. セル面積レポート ..... 49
6.7. 信号配線 ..... 50
6.8. ダミーメタル ..... 53
6.9. チップの方位合わせ ..... 54
6.10. 電源分離確認結果 ..... 57

**7. IR-DROP 検証 ..... 58**

**8. クロストークノイズ検証 ..... 59**

8.1. クロストークノイズ検証について ..... 59
8.2. 検証結果 ..... 59

**9. STA 検証 ..... 62**

9.1. 検証条件と結果 ..... 62
9.2. CLOCK GATING TIMING ERROR 概要 ..... 62
9.3. 最大動作速度 ..... 64
9.4. NOT ANNOTATED 解析 ..... 65

**10. 形式検証 ..... 65**

**11. レイアウト検証 ..... 67**

11.1. DRC ..... 67
11.2. ANT ..... 68
11.3. DFM ..... 69
11.4. FL ..... 70
11.5. LVS ..... 71

**12. 検証結果のまとめ ..... 72**

**13. 暗号ハードウェア IP コア ..... 73**

13.1. AES0 (合成体 S-BOX) ..... 73
13.2. AES1/AES2/AES3/AES4 (各種 S-BOX 実装) ..... 77
13.3. AES5 (CTR モード) ..... 79
13.4. AES6 (FA 対策版) ..... 85
13.5. AES7 (ラウンド鍵事前生成) ..... 89
13.6. AES8 (MAO) ..... 91
13.7. AES9 (MDPL) ..... 92
13.8. AES10 (THRESHOLD IMPLEMENTATION) ..... 93
13.9. AES11 (WDDL) ..... 93
13.10. AES12/AES13 (疑似 RSL) ..... 94
13.11. CAMELLIA ..... 95
13.12. CAST-128 ..... 98
13.13. DES ..... 101
13.14. ECC ..... 104
13.15. MISTY1 ..... 108
13.16. RSA ..... 110
13.17. SEED ..... 115
13.18. TDES ..... 118
13.19. CLEFIA ..... 121

**文献 ..... 124**

# 1. 概要

「サイドチャネル攻撃対策を施した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), および各種の暗号アルゴリズムを実装した LSI である. 暗号 LSI はイーシャトル社を経由し, 富士通マイクロエレクトロニクス社の 65nm プロセスで製造され, 160pin セラミック QFP に封止されている.

実装されている暗号アルゴリズムは 10 種類であり, AES については異なる 14 種類の実装形態があるため, 合計で 23 種類の暗号アルゴリズムコアを搭載している.

- 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
- RSA:1024bit のべき乗剰余演算
- ECC:鍵長は 64bit. 標数 2 の体における点のスカラー倍算
- CLEFIA:暗号化/復号サポート

主な機能は,

- 暗号アルゴリズムの実行
- 平成 18 年度に開発された FPGA 暗号評価基板(以下 SASEBO. )の制御用 FPGA 相当品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)

である.

## 2. 外部仕様

以下，暗号 LSI の外部仕様について述べる．

### 2.1. 入出力信号

表 2-1に暗号LSIの入出力信号を示す.

表 2-1 入出力信号

| 分類<br>(総数) | 信号名 | 本数 | 有意 | 方向<br>(LSI's view) | 用途・備考 |
|---|---|---|---|---|---|
| システム<br>(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<br>(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<br>(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[4:0] | 5 | -- | OUT | 選択 IP を示す |
| | MON[3:0] | 4 | -- | OUT | 内部モニタ用(詳細未定) |
| | | | | | |
| 計 | | 77 | | | |

### 2.2. ピンアサイン

暗号LSIのピンアサインを表 2-2に，TOP-VIEWのピンアサインイメージを図 2-1に示す．平成 20 年度に開発した暗号LSIでは，製造ルールが 130nmと 90nmであったため，ダイサイズが大きく，ダイのパッド数とパッケージピン数を共に 160 と等しくすることが可能であった．今回，製造ルールを 65nmとしたことで，ダイのパッド数は 136 に減少することとなった．このため，平成 20 年度に開発した暗号LSIのN．Cピンを活用すると共に，一部の電源ピンをダイに接続せずN．Cピン扱いにすることで，これまでの 160 ピンパッケージの暗号LSIとの互換性を確保している.

なお, 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ている.

表 2-2　暗号 LSI ピンアサイン (1/4)

| Pin NO | Signal Name | I/O | I/F Voltage | output | I/O Buffer | Function |
|---|---|---|---|---|---|---|
| 1 | VSS* | | | | | core GND |
| 2 | VSS* | | | | | core GND |
| 3 | VSS_IO | | | | | I/O GND |
| 4 | (SWIN[3]) | | | | | N.C |
| 5 | (SWIN[2]) | | | | | N.C |
| 6 | (SWIN[1]) | | | | | N.C |
| 7 | (SWIN[0]) | | | | | N.C |
| 8 | VDE | | | | | 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 | VSS_IO | | | | | 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 | VDE | | | | | I/O 3.3V |
| 20 | VDD | | | | | core 1.2V |
| 21 | VSS | | | | | core GND |
| 22 | VSS_IO | | | | | 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 | VSS_IO | | | | | I/O GND |
| 29 | A[15] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 30 | A[14] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 31 | A[13] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 32 | A[12] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 33 | VDE | | | | | I/O 3.3V |
| 34 | A[11] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 35 | A[10] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 36 | A[9] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 37 | A[8] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 38 | VSS_IO | | | | | I/O GND |
| 39 | VSS* | | | | | core GND |
| 40 | VSS* | | | | | core GND |

・「Signal Name」中の()は将来拡張用. 暗号 LSI では N.C ピン.

表 2-2 暗号 LSI ピンアサイン (2/4)

| Pin NO | Signal Name | I/O | I/F Voltage | output | I/O Buffer | Function |
|---|---|---|---|---|---|---|
| 41 | VDD | | | | | core 1.2V<br>(ダイには N.C) |
| 42 | VDE | | | | | I/O 3.3V<br>(ダイには N.C) |
| 43 | A[7] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 44 | A[6] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 45 | A[5] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 46 | A[4] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 47 | VSS_IO | | | | | I/O GND |
| 48 | VDD | | | | | core 1.2V |
| 49 | A[3] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 50 | A[2] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 51 | A[1] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 52 | A[0] | I | 3.3V | | IOCB2EITNNMXA02 | アドレスバス |
| 53 | VDE | | | | | I/O 3.3V |
| 54 | VSS | | | | | core GND |
| 55 | VSS_IO | | | | | I/O GND |
| 56 | CLKB | I | 3.3V | | IOCB2EITSNMXA02 | クロック.シュミット |
| 57 | VSS_IO | | | | | I/O GND |
| 58 | CLKA | I | 3.3V | | IOCB2EITSNMXA02 | クロック.シュミット |
| 59 | VSS_IO | | | | | I/O GND |
| 60 | VDD | | | | | core 1.2V |
| 61 | N.C | | | | | core GND |
| 62 | VSS | | | | | I/O GND |
| 63 | HRST_N | I | 3.3V | | IOCB2EITSNMXA02 | リセット.シュミット |
| 64 | N.C | | | | | I/O GND |
| 65 | WR_N | I | 3.3V | | IOCB2EITNNMXA02 | 書き込み指示 |
| 66 | RD_N | I | 3.3V | | IOCB2EITNNMXA02 | 読み出し指示 |
| 67 | VDE | | | | | I/O 3.3V |
| 68 | VSS | | | | | core GND |
| 69 | DO[15] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 70 | DO[14] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 71 | DO[13] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 72 | DO[12] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 73 | VSS_IO | | | | | I/O GND |
| 74 | VDD | | | | | core 1.2V |
| 75 | DO[11] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 76 | DO[10] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 77 | DO[9] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 78 | DO[8] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 79 | VDE | | | | | I/O 3.3V<br>(ダイには N.C) |
| 80 | VDD | | | | | core 1.2V<br>(ダイには N.C) |

・「Signal Name」 中の()は将来拡張用．暗号 LSI では N.C ピン．

表 2-2　暗号 LSI ピンアサイン(3/4)

| Pin NO | Signal Name | I/O | I/F Voltage | output | I/O Buffer | Function |
|---|---|---|---|---|---|---|
| 81 | VSS* | | | | | core GND |
| 82 | VSS* | | | | | core GND |
| 83 | VSS_IO | | | | | I/O GND |
| 84 | DO[7] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 85 | DO[6] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 86 | DO[5] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 87 | DO[4] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 88 | VDE | | | | | I/O 3.3V |
| 89 | DO[3] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 90 | DO[2] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 91 | DO[1] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 92 | DO[0] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 出力データ |
| 93 | VSS_IO | | | | | 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 | VDE | | | | | I/O 3.3V |
| 100 | VDD | | | | | core 1.2V |
| 101 | VSS | | | | | core GND |
| 102 | VSS_IO | | | | | 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 | VSS_IO | | | | | I/O GND |
| 109 | DI[0] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 110 | DI[1] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 111 | DI[2] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 112 | DI[3] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 113 | VDE | | | | | I/O 3.3V |
| 114 | DI[4] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 115 | DI[5] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 116 | DI[6] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 117 | DI[7] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 118 | VSS_IO | | | | | I/O GND |
| 119 | VSS* | | | | | core GND |
| 120 | VSS* | | | | | core GND |

・「Signal Name」中の()は将来拡張用．暗号 LSI では N.C ピン．

表 2-2　暗号 LSI ピンアサイン (4/4)

| Pin NO | Signal Name | I/O | I/F Voltage | output | I/O Buffer | Function |
|---|---|---|---|---|---|---|
| 121 | VDD* | | | | | core 1.2V |
| 122 | VDE* | | | | | I/O 3.3V |
| 123 | DI[8] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 124 | DI[9] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 125 | DI[10] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 126 | DI[11] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 127 | VSS_IO | | | | | I/O GND |
| 128 | VDD | | | | | core 1.2V |
| 129 | DI[12] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 130 | DI[13] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 131 | DI[14] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 132 | DI[15] | I | 3.3V | | IOCB2EITNNMXA02 | 入力データ |
| 133 | VDE | | | | | I/O 3.3V |
| 134 | VSS | | | | | core GND |
| 135 | (LED[0]) | | | | | N.C |
| 136 | (LED[1]) | | | | | N.C |
| 137 | END_N | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | ターゲット処理完了 |
| 138 | START_N | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | ターゲット処理開始 |
| 139 | VSS_IO | | | | | I/O GND |
| 140 | VDD | | | | | core 1.2V |
| 141 | VSS | | | | | core GND |
| 142 | VSS_IO | | | | | I/O GND |
| 143 | STATE[0] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 選択 IP を示す |
| 144 | STATE[1] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 選択 IP を示す |
| 145 | STATE[2] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 選択 IP を示す |
| 146 | STATE[3] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 選択 IP を示す |
| 147 | VDE | | | | | I/O 3.3V |
| 148 | VSS | | | | | core GND |
| 149 | STATE[4] | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | 選択 IP を示す |
| 150 | (MON[1]) | | | | | N.C |
| 151 | (MON[2]) | | | | | N.C |
| 152 | (MON[3]) | | | | | N.C |
| 153 | VSS_IO | | | | | I/O GND |
| 154 | VDD | | | | | core 1.2V |
| 155 | EXEC | O | 3.3V | 8mA | IOCB2EOT2X8NA02 | ターゲット処理中 |
| 156 | N.C | | | | | N.C |
| 157 | N.C | | | | | N.C |
| 158 | N.C | | | | | N.C |
| 159 | VDE* | | | | | I/O 3.3V |
| 160 | VDD* | | | | | core 1.2V |

・「Signal Name」 中の( )は将来拡張用．暗号 LSI では N.C ピン.

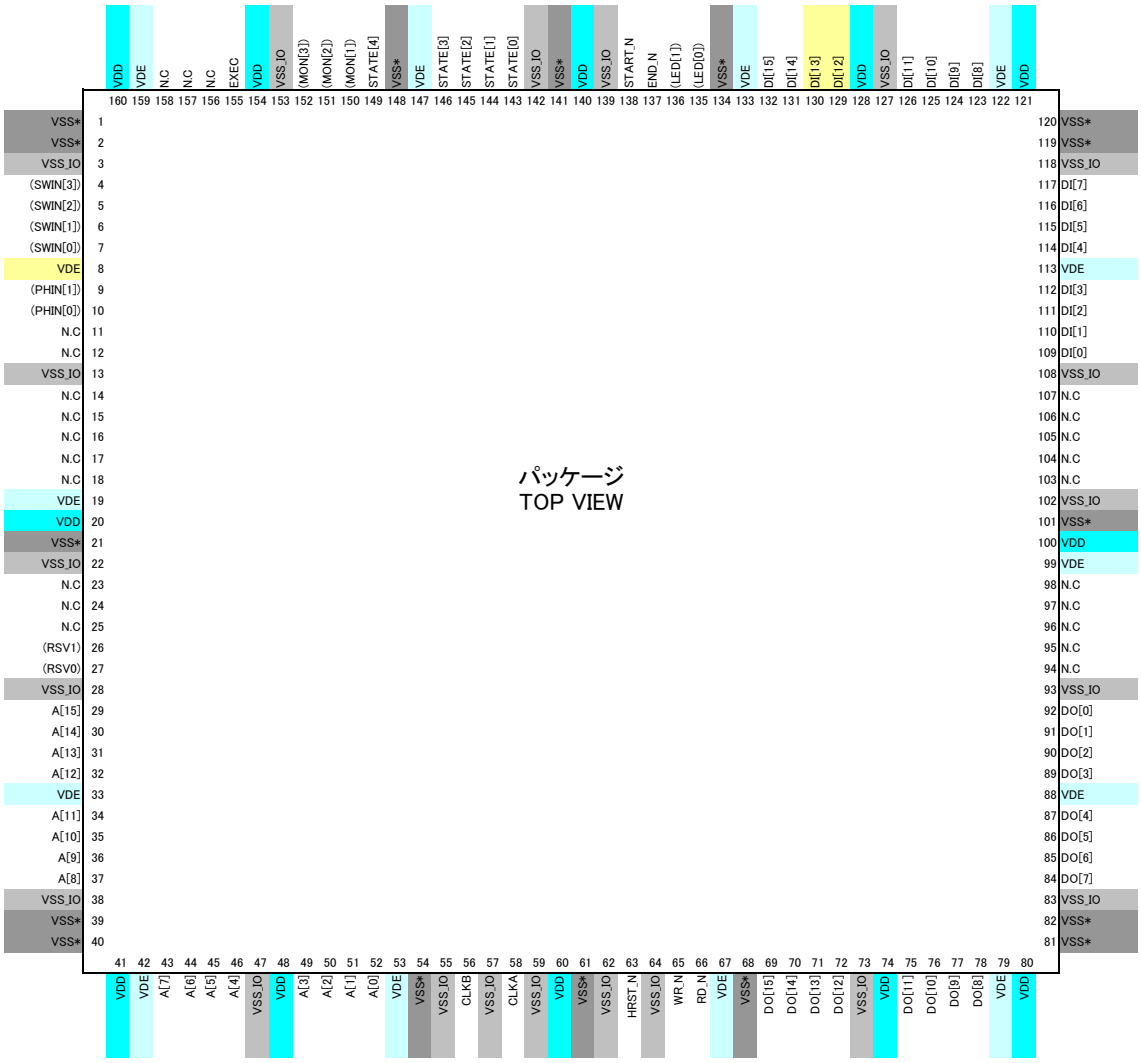



図 2-1　暗号 LSI ピンアサインイメージ

## 2.3. 入出力タイミング

暗号LSIの入出力タイミングを図 2-2～図 2-4に示す.

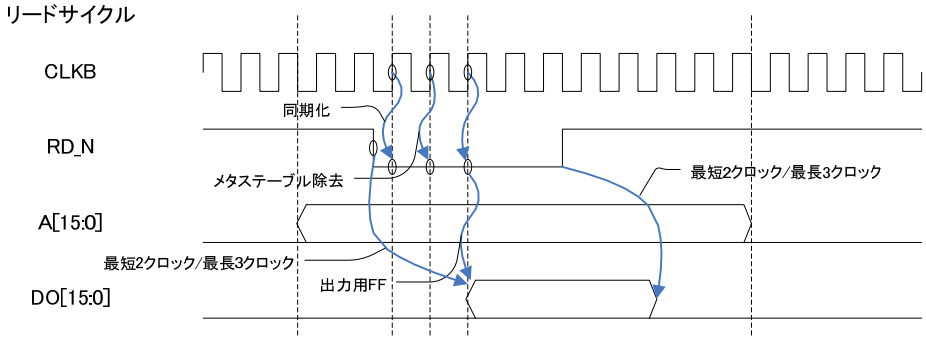



図 2-2　リードサイクルタイミングチャート

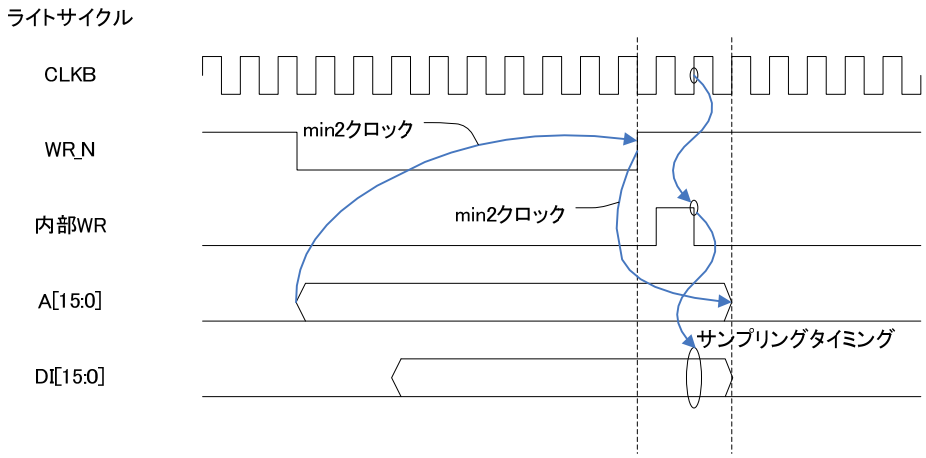



図 2-3　ライトサイクルタイミングチャート

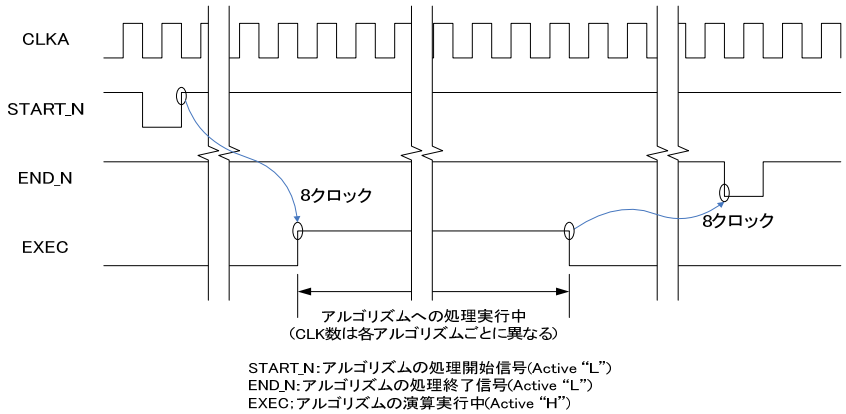



図 2-4　評価用タイミング信号

## 2.4. インタフェースレジスタ

暗号LSIのインタフェースレジスタ，およびアドレスマップの一覧を表 2-3に示す.

表 2-3　インタフェースレジスタ (1/2)

| 分類 | | アドレス | レジスタ名 | 略称 | R/W | 機能など |
|---|---|---|---|---|---|---|
| システム制御 | | 0x0000 | (予約) | | -- | |
| | | 0x0002 | 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)<br>鍵生成の指示(W)/終了の通知(R)<br>暗号 IP のリセット制御(W) |
| | | 0x0004 | IP 選択レジスタ 0 | IPSEL0 | R/W | 動作させる暗号 IP を指定 |
| | | 0x0006 | IP 選択レジスタ1 | IPSEL1 | R/W | 動作させる暗号 IP を指定 |
| | | 0x0008 | 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 |
| | | 0x000A | 出力選択レジスタ 1 | OUTSEL1 | R/W | データ出力する暗号 IP を指定 |
| | | 0x000C | ﾓｰﾄﾞﾚｼﾞｽﾀ | MODE | R/W | 動作モード，鍵長，暗復号などを指定 |
| | | 0x000E | 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 |
| | | 0x0010 | テストレジスタ 1 | TEST1 | R | カスタムコア動作制御 1 |
| | | 0x0012 | テストレジスタ 2 | TEST2 | R | カスタムコア動作制御 2 |
| | | :<br>0x00FF | (予約) | | | |
| 共通鍵暗号 | 秘密鍵<br>(→暗号 LSI) | 0x0100 | 鍵レジスタ 0 | KEY0 | W | 共通鍵暗号用鍵(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0102 | 鍵レジスタ 1 | KEY1 | W | 共通鍵暗号用鍵(KEY0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x010E | 鍵レジスタ 7 | KEY7 | W | 共通鍵暗号用鍵(最下位 16 ﾋﾞｯﾄ) |
| | IV<br>(→暗号 LSI) | 0x0110 | IV データレジスタ 0 | IV0 | W | 入力 IV データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0112 | IV データレジスタ 1 | IV 1 | W | 入力 IV データ(IV0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x011E | IV ﾃﾞｰﾀﾚｼﾞｽﾀ 7 | IV 7 | W | 入力 IV データ(最下位 16 ﾋﾞｯﾄ) |
| | 入力テキスト<br>(→暗号 LSI) | 0x0120 | 入力テキストレジスタ 0 | ITEXT0 | W | 入力テキストデータ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0122 | 入力テキストレジスタ 1 | ITEXT1 | W | 入力テキストデータ(ITEXT0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x015E | 入力テキストレジスタ 31 | ITEXT31 | W | 入力テキストデータ(最下位 16 ﾋﾞｯﾄ) |
| | 乱数データ<br>(→暗号 LSI) | 0x0160 | 乱数データレジスタ 0 | RAND0 | W | 入力乱数データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0162 | 乱数データレジスタ 1 | RAND1 | W | 入力乱数データ(RAND0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x016E | 乱数データレジスタ 7 | RAND7 | W | 入力乱数データ(最下位 16 ﾋﾞｯﾄ) |
| | (予約) | :<br>0x017E | (予約) | | | |
| | 出力テキスト<br>(←暗号 LSI) | 0x0180 | 出力テキストレジスタ 0 | OTEXT0 | R | 出力テキストデータ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0182 | 出力テキストレジスタ 1 | OTEXT1 | R | 出力テキストデータ(OTEXT0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x01BE | 出力テキストレジスタ 31 | OTEXT31 | R | 出力テキストデータ(最下位 16 ﾋﾞｯﾄ) |
| | 中間値データ<br>(←暗号 LSI) | 0x01C0 | 中間値レジスタ 0 | RDATA0 | R | 中間値データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x01C2 | 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) |
| | | : | : | : | : | : |
| | | 0x01CE | 中間値レジスタ 7 | RDATA7 | R | |
| | 中間鍵データ<br>(←暗号 LSI) | 0x01D0 | 中間鍵レジスタ 0 | RKEY0 | R | 中間鍵データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x01D2 | 中間鍵レジスタ 1 | RKEY1 | R | 中間鍵データ(RKEY0 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x01DE | 中間鍵レジスタ 7 | RKEY7 | R | 中間鍵データ(最下位 16 ﾋﾞｯﾄ) |
| | (予約) | :<br>0x01FE | (予約) | | | |

表 2-3　インタフェースレジスタ(2/2)

| 分類 | | アドレス | レジスタ名 | 略称 | R/W | 機能など |
|---|---|---|---|---|---|---|
| 公開鍵暗号 | 指数<br>(←暗号 LSI)<br>(*1) | 0x0200 | 指数レジスタ 0 | EXP00 | W | 指数(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0202 | 指数レジスタ 1 | EXP01 | W | 指数(EXP00 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x023E | 指数レジスタ 31 | EXP1F | W | 指数(最下位 16 ﾋﾞｯﾄ) |
| | | :<br>0x02FE | (予約) | | | |
| | 法<br>(→暗号 LSI)<br>(*2) | 0x0300 | 法レジスタ 0 | MOD00 | W | 法(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0302 | 法レジスタ 1 | MOD01 | W | 法(MOD00 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x033E | 法レジスタ 31 | MOD1F | W | 法(最下位 16 ﾋﾞｯﾄ) |
| | | :<br>0x037E | (予約) | | | |
| | 前処理演算結果入力<br>(→暗号 LSI)<br>(*3) | 0x0380 | 前処理演算結果レジスタ 0 | PREDAT00 | W | 前処理演算結果(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0382 | 前処理演算結果レジスタ 1 | PREDAT01 | W | 前処理演算結果(PREDAT00 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x039E | 前処理演算結果レジスタ 16 | PREDAT0F | W | 前処理演算結果(最下位 16 ﾋﾞｯﾄ) |
| | | :<br>0x03FE | (予約) | | | |
| | 入力データ<br>(→暗号 LSI)<br>(*4) | 0x0400 | 入力データレジスタ 0 | IDATA00 | W | 入力データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0402 | 入力データレジスタ 1 | IDATA01 | W | 入力データ(IDATA00 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x043E | 入力データレジスタ 31 | IDATA1F | W | 入力データ(最下位 16 ﾋﾞｯﾄ) |
| | | :<br>0x04FE | (予約) | | | |
| | 出力データ<br>(←暗号 LSI)<br>(*5) | 0x0500 | 出力データレジスタ 0 | ODATA00 | R | 出力データ(最上位 16 ﾋﾞｯﾄ) |
| | | 0x0502 | 出力データレジスタ 1 | ODATA01 | R | 出力データ(ODATA00 に続く 16 ﾋﾞｯﾄ) |
| | | : | : | : | : | : |
| | | 0x053E | 出力データレジスタ 31 | ODATA1F | R | 出力データ(最下位 16 ﾋﾞｯﾄ) |
| | | :<br>0x05FE | (予約) | | | |
| (空き) | | 0x0600<br>:<br>0xFFEE | | | | |
| チップ情報<br>(0xFFF0<br>～0xFFFF) | | 0xFFF0<br>: | (予約) | | | |
| | | 0xFFFC | バージョンレジスタ | VER | R | |
| | | 0xFFFE | (予約) | | -- | |

(*1) ECC の場合は、鍵及び乱数用レジスタとなり以下の範囲
0x0200-0x0206 指数レジスタ 0-3 EXP00-03 鍵レジスタ 64bit
0x0208-0x020e 指数レジスタ 4-7 EXP04-07 乱数レジスタ 64bit
(*2) ECC の場合は、ECC の初期点の x 座標レジスタとなり以下の範囲
0x0300-0x0316 法レジスタ 0-11 MOD00-0B x 座標レジスタ 192bit
(*3) ECC の場合は、ECC の Z 座標レジスタとなり以下の範囲
0x0380-0x0396 前処理演算結果レジスタ 0-11 PREDAT00-0B Z 座標レジスタ 192bit
(*4) ECC の場合は、ECC のパラメータ b レジスタとなり以下の範囲
0x0400-0x0416 入力データレジスタ 0-11 IDATA00-0B パラメータ b レジスタ 192bit
(*5) ECC の場合は、ECC の出力データレジスタとなり以下の範囲
0x0500-0x0516 出力データレジスタ 0-11 ODATA00-0B 出力データレジスタ 192bit

## 2.5. 動作手順

インタフェースレジスタにより，暗号アルゴリズムコアに処理を行わせる手順を以下に示す.

(1)AES5(CTR モードサポートパイプライン実装)以外の暗号アルゴリズムコア以外

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 EXP00-1F と MOD00-1F, ECC は IDATA00-03 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 ：
　⑧-1　共通鍵暗号は ITEXT0-7(*4)，RSA は IDATA00-1F，ECC は IDATA08-13 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 ODATA00-1F，ECC は ODATA00-03 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(故障攻撃耐性評価用実装)選択時は，RDATA0-7/RKEY0-7 を読み出すことも出来る.(ラウンド選択レジスタに設定したラウンド数，若しくは，fault 発生時の中間値を読み出せる.)

設定の変更は以下の手順による.
・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.

(2)AES5(CTR モードサポートパイプライン実装)コア

※鍵設定までは(1)の手順と同一である.

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　：

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.

# 3. 詳細仕様

以下より，評価 LSI の詳細な内部仕様について説明する．評価 LSI では実際に暗号アルゴリズムを処理する暗号アルゴリズムコアは，産総研殿よりリリース頂いたものを組み込んでいる．このため，本章では各暗号アルゴリズムの詳細については，概要程度に留めて LSI 外部や各暗号アルゴリズムコアとのインタフェースに重点を置いている点に留意されたい．

## 3.1. 全体ブロック図

本節では，暗号LSIの全体構成について説明する．図 3-1に暗号LSIの全体ブロックを示す．


図 3-1　全体ブロック図

## 3.2. 階層構造

暗号LSIの階層構造を図 3-2に示す．

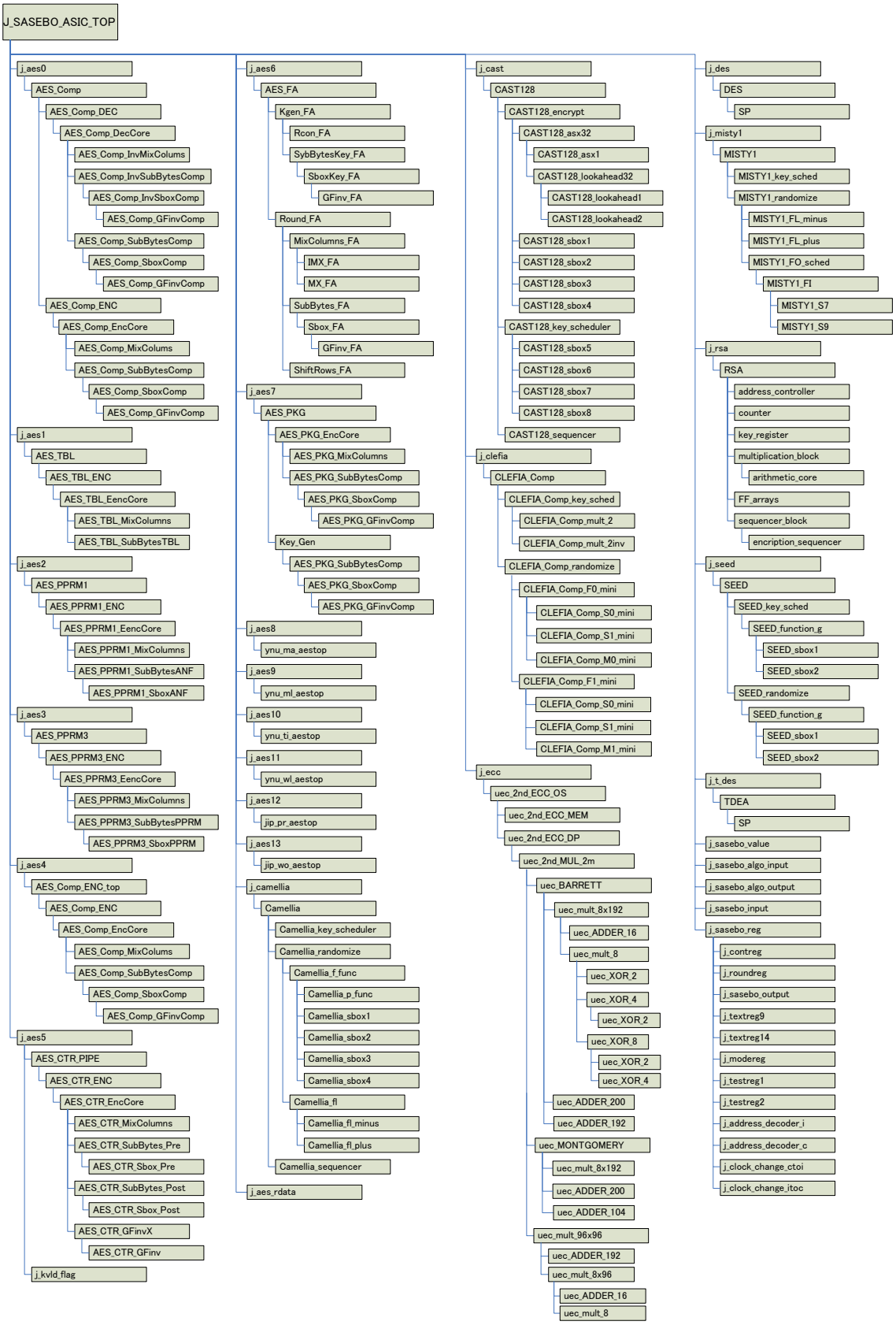
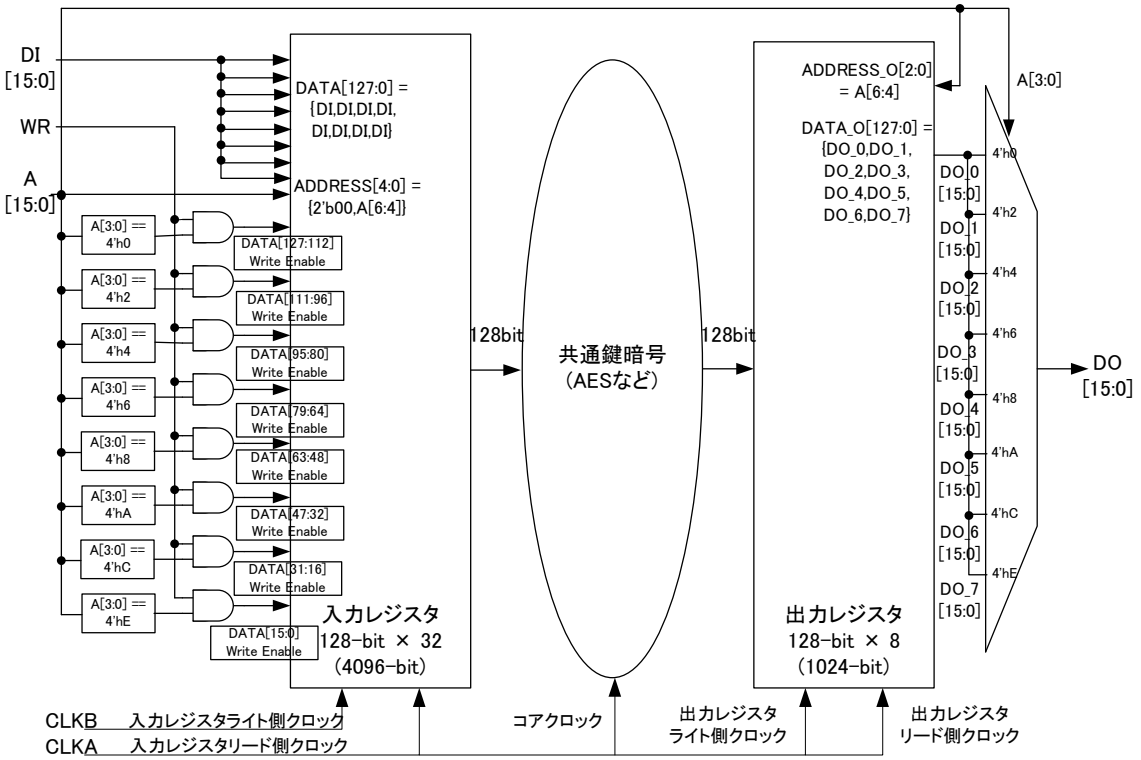

J_SASEBO_ASIC_TOP
j_aes0
AES_Comp
AES_Comp_DEC
AES_Comp_DecCore
AES_Comp_InvMixColums
AES_Comp_InvSubBytesComp
AES_Comp_InvSboxComp
AES_Comp_GFinvComp
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColums
AES_Comp_SubBytesComp
AES_Comp_SboxComp
AES_Comp_GFinvComp
j_aes1
AES_TBL
AES_TBL_ENC
AES_TBL_EencCore
AES_TBL_MixColumns
AES_TBL_SubBytesTBL
j_aes2
AES_PPRM1
AES_PPRM1_ENC
AES_PPRM1_EencCore
AES_PPRM1_MixColumns
AES_PPRM1_SubBytesANF
AES_PPRM1_SboxANF
j_aes3
AES_PPRM3
AES_PPRM3_ENC
AES_PPRM3_EencCore
AES_PPRM3_MixColumns
AES_PPRM3_SubBytesPPRM
AES_PPRM3_SboxPPRM
j_aes4
AES_Comp_ENC_top
AES_Comp_ENC
AES_Comp_EncCore
AES_Comp_MixColums
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
Kgen_FA
Rcon_FA
SybBytesKey_FA
SboxKey_FA
GFinv_FA
Round_FA
MixColumns_FA
IMX_FA
MX_FA
SubBytes_FA
Sbox_FA
GFinv_FA
ShiftRows_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_key_scheduler
Camellia_randomize
Camellia_f_func
Camellia_p_func
Camellia_sbox1
Camellia_sbox2
Camellia_sbox3
Camellia_sbox4
Camellia_fl
Camellia_fl_minus
Camellia_fl_plus
Camellia_sequencer
j_aes_rdata
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_clefia
CLEFIA_Comp
CLEFIA_Comp_key_sched
CLEFIA_Comp_mult_2
CLEFIA_Comp_mult_2inv
CLEFIA_Comp_randomize
CLEFIA_Comp_F0_mini
CLEFIA_Comp_S0_mini
CLEFIA_Comp_S1_mini
CLEFIA_Comp_M0_mini
CLEFIA_Comp_F1_mini
CLEFIA_Comp_S0_mini
CLEFIA_Comp_S1_mini
CLEFIA_Comp_M1_mini
j_ecc
uec_2nd_ECC_OS
uec_2nd_ECC_MEM
uec_2nd_ECC_DP
uec_2nd_MUL_2m
uec_BARRETT
uec_mult_8x192
uec_ADDER_16
uec_mult_8
uec_XOR_2
uec_XOR_4
uec_XOR_2
uec_XOR_8
uec_XOR_2
uec_XOR_4
uec_ADDER_200
uec_ADDER_192
uec_MONTGOMERY
uec_mult_8x192
uec_ADDER_200
uec_ADDER_104
uec_mult_96x96
uec_ADDER_192
uec_mult_8x96
uec_ADDER_16
uec_mult_8
j_des
DES
SP
j_misty1
MISTY1
MISTY1_key_sched
MISTY1_randomize
MISTY1_FL_minus
MISTY1_FL_plus
MISTY1_FO_sched
MISTY1_FI
MISTY1_S7
MISTY1_S9
j_rsa
RSA
address_controller
counter
key_register
multiplication_block
arithmetic_core
FF_arrays
sequencer_block
encription_sequencer
j_seed
SEED
SEED_key_sched
SEED_function_g
SEED_sbox1
SEED_sbox2
SEED_randomize
SEED_function_g
SEED_sbox1
SEED_sbox2
j_t_des
TDEA
SP
j_sasebo_value
j_sasebo_algo_input
j_sasebo_algo_output
j_sasebo_input
j_sasebo_reg
j_contreg
j_roundreg
j_sasebo_output
j_textreg9
j_textreg14
j_modereg
j_testreg1
j_testreg2
j_address_decoder_i
j_address_decoder_c
j_clock_change_ctoi
j_clock_change_itoc

図 3-2 階層構造

## 3.3. 外部インタフェース回路

共通鍵系暗号アルゴリズム (AES, DES, MISTY1, Camellia, SEED, CAST128, CLEFIA)と公開鍵系暗号アルゴリズム(RSA, ECC)に分けて外部インタフェース回路について説明する.
図 3-3に共通鍵系暗号アルゴリズムの外部インタフェース回路を, 図 3-4に公開鍵系暗号アルゴリズムの外部インタフェース回路を示す.

＜共通鍵用のRegisterについて＞




【メモリマップ】

①入力レジスタ

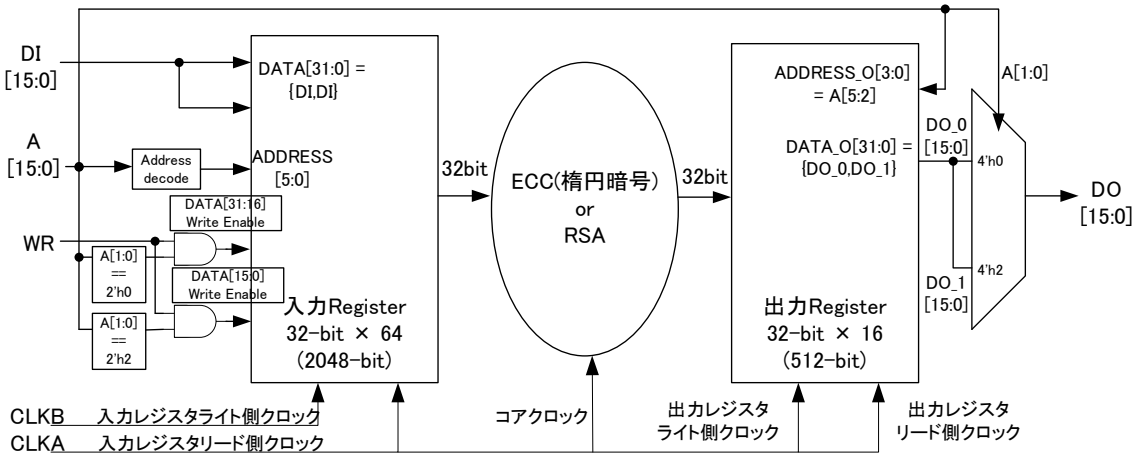
| | | |
|---|---|---|
| 127 | 秘密鍵 128bit | 0 |
| 127 | IV 128bit | 0 |
| 127 | | 0 |
| 127 | 入力テキスト | 0 |
| 127 | 128bit×4 | 0 |
| 127 | | 0 |
| 127 | 乱数データ 128bit | 0 |
| 未使用 3200bit | | |

②出力レジスタ

| | | |
|---|---|---|
| 127 | | 0 |
| 127 | 出力テキスト | 0 |
| 127 | 128bit×4 | 0 |
| 127 | | 0 |
| 127 中間値データ 128bit | | 0 |
| 127 中間鍵データ 128bit | | 0 |
| 未使用 128bit | | |

図 3-3　共通鍵系暗号アルゴリズムインタフェース回路

＜RSA及びECC用Registerについて＞




【メモリマップ】

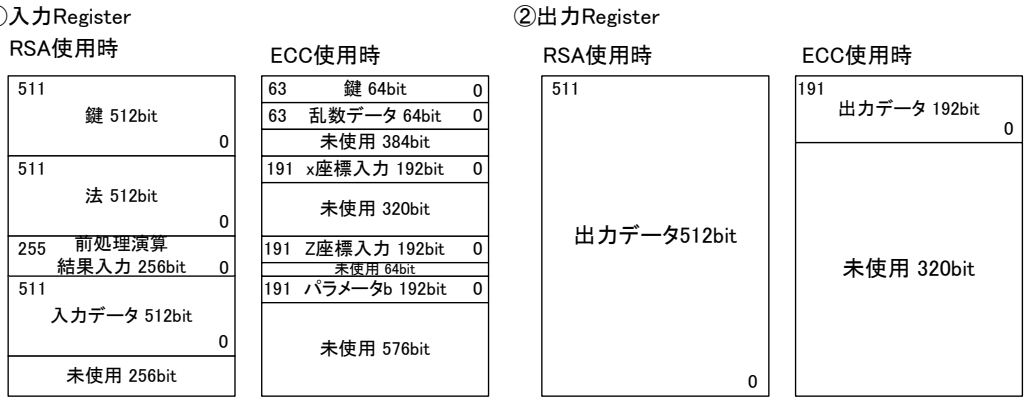



図 3-4　公開鍵系暗号アルゴリズムインタフェース回路

## 3.4. 暗号アルゴリズムコアインタフェース

本章では各暗号アルゴリズムコアとのインタフェースについて，鍵スケジュールや暗号処理に要するサイクル数などについて簡単に説明する.

(0) AES0
- ・S-Box 構造:合成体
- ・鍵スケジュールサイクル数:暗号化時 1[cycle]/復号時:11[cycle]
- ・暗号化/復号処理サイクル:10[cycle/block]
- ・備考:暗号化/復号処理サポート.

(1) AES1
- ・S-Box 構造:case 文記述によるテーブル実装
- ・鍵スケジュールサイクル数:1[cycle]
- ・暗号化処理サイクル:10[cycle/block]
- ・備考:暗号化のみサポート.

(2) AES2
・S-Box 構造:AND-XOR 構造 1 段で記述
・鍵スケジュールサイクル数:1[cycle]
・暗号化処理サイクル:10[cycle/block]
・備考:暗号化のみサポート.
(3) AES3
・S-Box 構造:AND-XOR 構造3段で記述
・鍵スケジュールサイクル数:1[cycle]
・暗号化処理サイクル:10[cycle/block]
・備考:暗号化のみサポート.
(4) AES4
・S-Box 構造:合成体
・鍵スケジュールサイクル数:1[cycle]
・暗号化処理サイクル:10[cycle/block]
・備考:暗号化のみサポート.
(5) AES5
・S-Box 構造:合成体
・鍵スケジュールサイクル数:1[cycle]
・暗号化処理サイクル:46[cycle/4block]
・備考:CTR モード回路を含む 1round/4stage のインナーパイプライン実装.
(6) AES6
・S-Box 構造:合成体
・鍵スケジュールサイクル数:20[cycle]/21[cycle](暗号化/復号)
・暗号化処理サイクル:21[cycle/block]
・備考:フォルト攻撃対策を施した AES 実装. 暗号化/復号サポート.
(7) AES7
・S-BOX 構造:合成体
・鍵スケジュールサイクル数:11[cycle]
・暗号化/復号処理サイクル:10[cycle/block]
・備考:ラウンド鍵を事前計算する AES 実装. 暗号化のみサポート.
(8) AES8
・DPA 対策評価用実装(Masked AND Operation)
(9) AES9
・DPA 対策評価用実装(MDPL)
(10) AES10
・DPA 対策評価用実装(WDDL)
(11) AES11
・DPA 対策評価用実装(Masked AND Operation)
(12) AES12
・DPA 対策評価用実装(擬似 RSL)
(13) AES13
・DPA 対策評価用実装(擬似 RSL の効果評価用)
(14) Camellia
・鍵スケジュールサイクル数:6[cycle]
・暗号化/復号処理サイクル:23[cycle/block]
・備考:暗号化/復号をサポート.

(15) SEED
・鍵スケジュールサイクル数：1[cycle]
・暗号化/復号処理サイクル：16[cycle/block]
・備考：暗号化/復号をサポート.
(16) MISTY1
・鍵スケジュールサイクル数：8[cycle]
・暗号化/復号処理サイクル：9[cycle/block]
・備考：暗号化/復号をサポート.
(17) Triple-DES
・鍵スケジュールサイクル数：1[cycle]
・暗号化/復号処理サイクル：48[cycle/block]
・備考：暗号化/復号をサポート.
(18) DES
・鍵スケジュールサイクル数：1[cycle]
・暗号化/復号処理サイクル：16[cycle/block]
・備考：暗号化/復号をサポート.
(19) CAST128
・鍵スケジュールサイクル数：128[cycle]
・暗号化/復号処理サイクル：16[cycle/block]
・備考：暗号化/復号をサポート.
(20) RSA
・RSA 暗号のべき乗剰余演算処理を実行する.
・6 種類のべき乗剰余演算アルゴリズム（左バイナリ法，対策版左バイナリ法，右バイナリ法，対策版右バイナリ法，Montgomery Powering Ladder，M. Joye の右バイナリ法）および CRT 演算をサポート.
・サイドチャネル攻撃対策として”square-and-multiply always method”（ダミー演算による対策法），Montgomery Powering Ladder および M. Joye の提案する右バイナリ法をサポート.
・乗剰余演算には高基数モンゴメリ乗算アルゴリズムを使用.
(21) ECC
・標数 2 の体における点の倍算をおこない，鍵サイズは 64bit までサポート.
・点の倍算はロペスとダハブの提案したアルゴリズムに従う.
(22) CLEFIA
・鍵スケジュールサイクル数：13[cycle]
・暗号化処理サイクル：18[cycle/block]
・復号処理サイクル：19[cycle/block]
・備考：暗号化/復号をサポート.

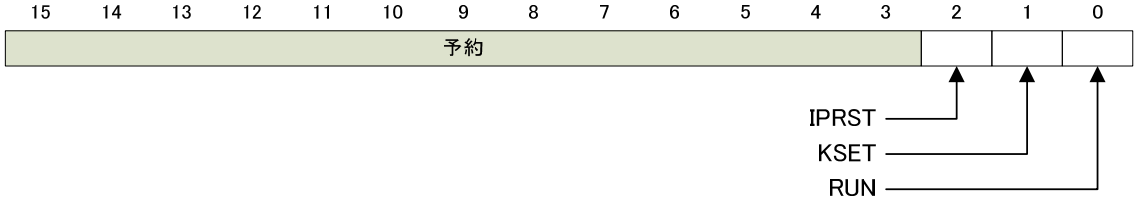
## 3.5. インタフェースレジスタ詳細

本節ではインタフェースレジスタの詳細について説明する.

### 3.5.1. システム制御レジスタ群

①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.




ビット 0:RUN

1 を書き込むと 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タフェースクロック CLK_B から内部クロック CLK_A へ同期化した後, CLK_A で 16 クロック後の暗号 IP の動作を開始する.
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/データレジスタの読み出し値は無意味である.

ビット 1:KSET

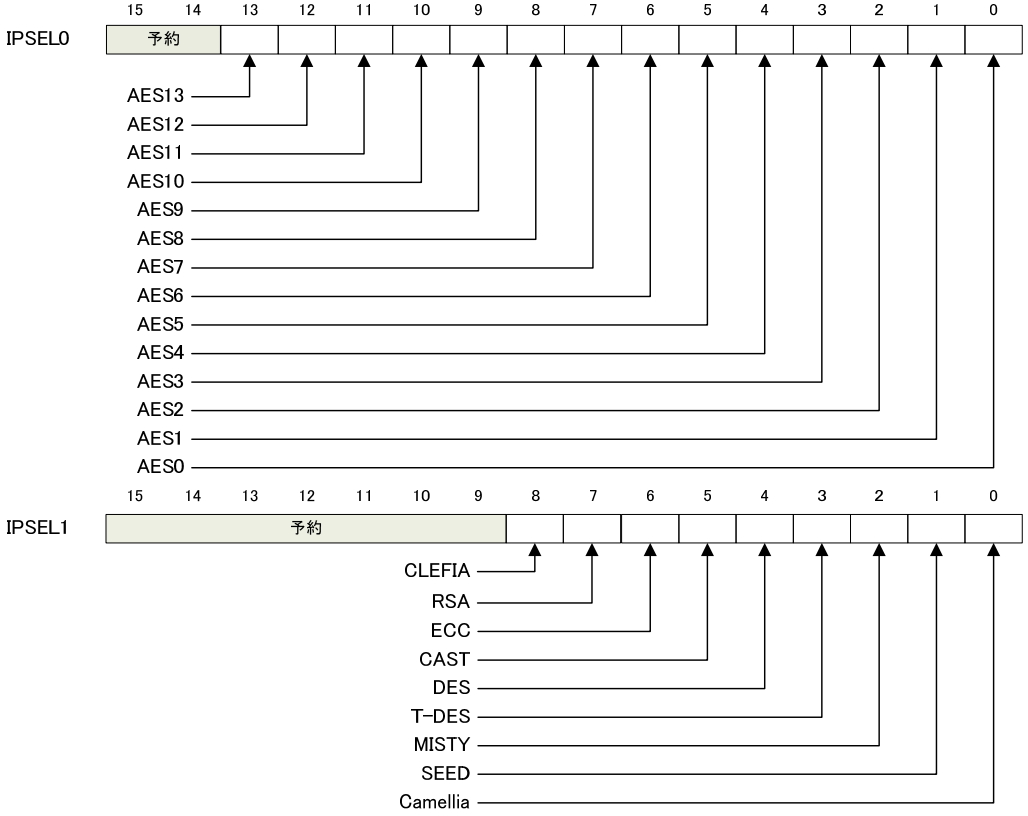
1 を書き込むと IP 選択レジスタ(IPSEL)で指定した暗号 IP に, モードレジスタ:MODE に応じた鍵生成(鍵設定)が行われる.
出力選択レジスタ(OUTSEL)で指定した暗号 IP の鍵生成(鍵設定)が終了し, 設定された鍵を用いた暗号処理が可能になると, 本ビットは自動的に 0 クリアされる.
本ビットが 1 の期間中は, 全てのレジスタへの書き込みは原則禁止とする.(特に, 本ビットが 1 の期間中に RUN ビットをセットした場合の動作は保証しない.)

ビット 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.

②IP 選択レジスタ:IPSEL0, 1

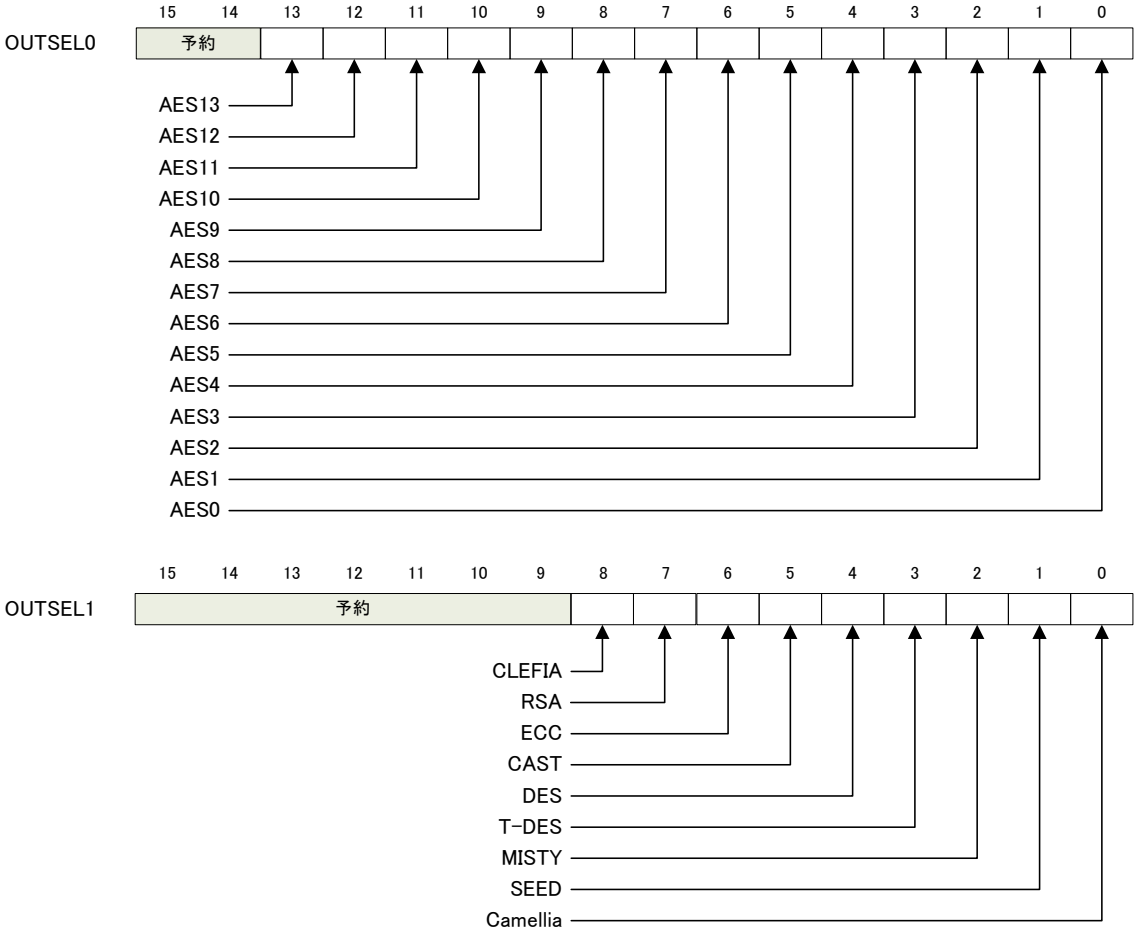
ASIC に搭載される複数の暗号 IP のうち, IP 選択レジスタの対応するビットに 1 がセットされたもののみが active 状態となる. 選択 IP 以外にはクロックが供給されない.



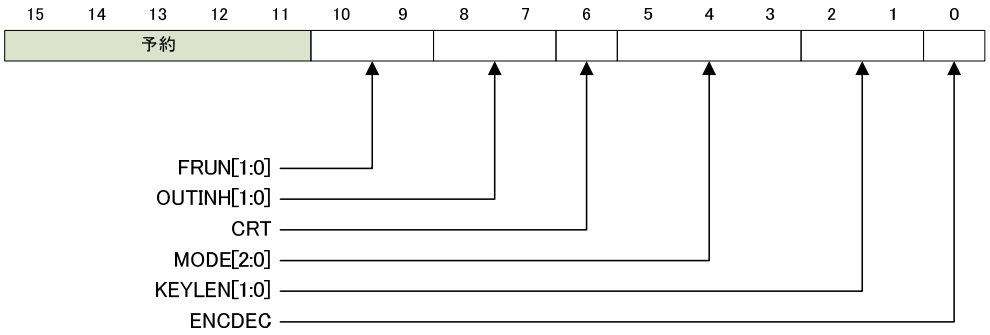

| ビット | 暗号 IP | 備考 |
|---|---|---|
| AES0 | S-Box 実装→合成体, 暗号化/復号サポート | AES_Comp |
| AES1 | S-Box 実装→case 文記述, 暗号化のみサポート | AES_TBL |
| AES2 | S-Box 実装→AND-XOR 実装(1-Stage), 暗号化のみサポート | AES_PPRM1 |
| AES3 | S-Box 実装→AND-XOR 実装(3-Stage), 暗号化のみサポート | AES_PPRM3 |
| AES4 | S-Box 実装→合成体, 暗号化のみサポート | AES_Comp_ENC_top |
| AES5 | CTR モードサポートパイプライン実装 | AES_CTR_PIPE |
| AES6 | 故障攻撃耐性評価用実装 | AES_FA |
| AES7 | ラウンド鍵を事前計算する実装 | AES_PKG |
| AES8 | DPA 対策評価用実装(Masked AND Operation) | |
| AES9 | DPA 対策評価用実装(MDPL) | |
| AES10 | DPA 対策評価用実装(Threshold Implementation) | |
| AES11 | DPA 対策評価用実装(WDDL) | |
| AES12 | DPA 対策評価用実装(擬似 RSL) | |
| AES13 | DPA 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 | SEED:暗号化/復号サポート | |
| MISTY | MISTY1:暗号化/復号サポート | |
| T_DES | Triple-DES:3Key, 暗号化/復号サポート | |
| DES | 暗号化/復号サポート | |
| CAST | 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 | RSA:1024bit のべき乗剰余演算 | |
| CLEFIA | CLEFIA:暗号化/復号サポート | |

③出力選択レジスタ:OUTSEL0, 1

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しない.



④モードレジスタ：MODE
　動作モード，鍵長，暗復号を指定する．

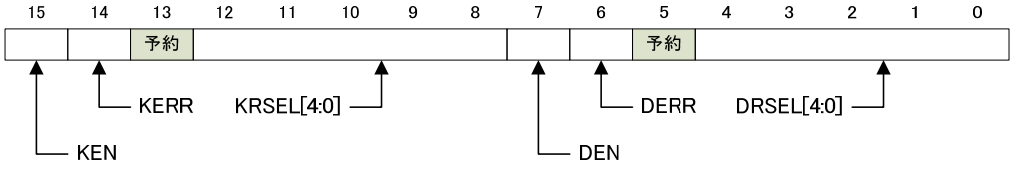



ビット 10-9：FRUN：フリーランモード制御(AES0 のみでサポート)(0.3 秒毎に 1 回実行)
　　FRUN[1]：　0　FRUN モード OFF
　　　　1　FRUN モード ON
　　FRUN[0]：　0　ITEXT を初期値に+1 インクリメントしながらフリーラン
　　　　1　ITEXT を初期値に暗号化結果を次回入力にしながらフリーラン
ビット 8-7：OUTINH：制御信号の出力抑止コントロール
　　OUTINH[1]：0　制御信号出力抑止機能 OFF(制御信号は出力される)
　　　　1　制御信号出力抑止機能 ON(内容は OUTINH[0]による)
　　OUTINH[0]：0　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
ビット 6：CRT：RSA 以外意味を持たない．本ビットは RSA コアの CRT ポートに直結される．
　　0：CRT 処理 OFF
　　1：CRT 処理 ON
ビット 5-3：MODE
　　AES12 と RSA 以外：IP 毎に決まっている暗号利用モード又は動作モード
　　RSA：RSA の MODE 入力に直結する
　　　000：左バイナリ法
　　　001：右バイナリ法
　　　010：対策版左バイナリ法
　　　011：対策版右バイナリ法
　　　100：Montgomery Powering Ladder
　　　101：M.Joye の右バイナリ法
　　なお，AES12 の動作モードはテストレジスタ 2：TEST2 の設定に従う
　　ビット 2-1：KEYLEN（00 固定）：IP 毎に決まっている固定鍵長
　　ビット 0：ENCDEC
　　　0　暗号化
　　　1　復号
　　（暗号化のみの IP が選択された場合，ENCDEC ビットは意味を持たない）

⑤ラウンド選択レジスタ:RSEL

中間値レジスタ(RDATA0-RDATA7), 及び中間鍵レジスタ(RKEY0-RKEY7)に値を取り込むラウンド数を指定する.

KRSEL/RDATA0-RDATA7 及び DRSEL/RKEY0-RKEY7 は, active な暗号 IP として AES6 が選択されている時のみ意味を持つ.




ビット 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).

ビット 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

ビット 12-8:KRSEL

中間鍵レジスタ(RKEY0-RKEY7)に中間鍵データを格納すべきラウンド数.

ビット 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).

ビット 6: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

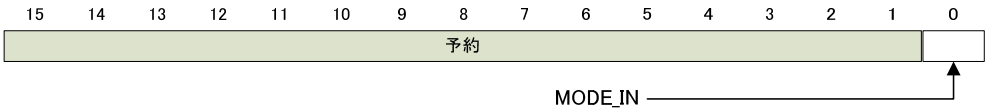
1 エラー発生

ビット 4-0:DRSEL

中間鍵レジスタ(RDATA0-RDATA7)に中間値データを格納すべきラウンド数.

⑥テストレジスタ 1:TEST1

テストレジスタ 1(TEST1)に 0x0001 を書くことで、外部から入力した鍵は使用せず、内部鍵を使用した暗号化が行われるようになる。一度、テストレジスタ 1に 0x0001 を書くと通常の外部から入力した鍵を使用した暗号処理に戻るためには、電源を落とす(もしくは、HRST_N をかける)必要がある。これをサポートしているのは、すべての AES(AES0-13)である。

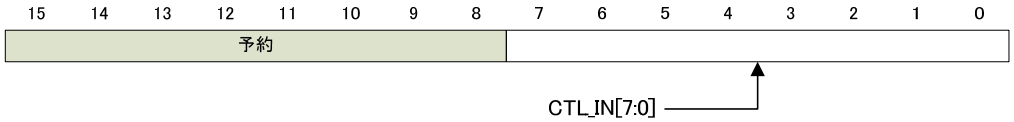



ビット 0:MODE_IN

⑦テストレジスタ 2:TEST2

テストレジスタ 2 は AES12 コアの制御を行うレジスタである. CTL_IN[7:0]は AES12 の ctl_in[7:0]信号にそのまま接続される.

ctl_in 信号の詳細については,「産業技術総合研究所殿向け耐タンパ性評価用暗号 IP 外部仕様」を参照のこと.




ビット 7-0:CTL_IN[7:0]

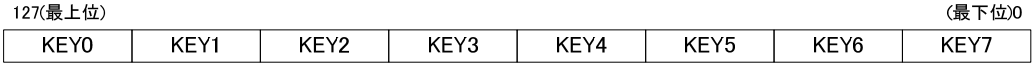
AES12 コアの ctl_in[7:0]信号の制御.

### 3.5.2. 共通鍵暗号用レジスタ群

①鍵レジスタ:KEY0-7

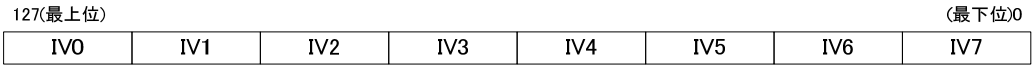
鍵レジスタ(KEY0-7)は, 128bit 分用意しているが, 暗号コアの演算では, KEY4 の下位 8bit と KEY5-7 の合計 56bit 分しか使用しない. 各暗号コアの鍵の取扱いは以下の通り.

- ・DES: パリティビットを含まない 56bit の鍵を KEY4 の下位 8bit 及び KEY5-7 に入力する. これら 56bit の鍵に対して回路中で, パリティビットを加えて DES の鍵として使用する.
- ・T-DES: パリティビットを含まない 56bit の鍵を KEY4 の下位 8bit と KEY5-7 に入力する. T-DES には, 以下のように入力される.
  - [191:64]: 0x00010203040506070809 0a0b0c0d0e0f (固定値)
  - [63:0]: 外部より入力された 56bit の鍵にパリティを追加したもの
- ・その他の共通鍵暗号:鍵が 128bit であるため以下のように入力している.
  - [127:56]: 0x00010203040506070 8
  - [55:0]: 外部より入力された鍵 (KEY4 の下位 8bit 及び KEY5-7 の 56bit 分)




②IVデータレジスタ:IV0-7

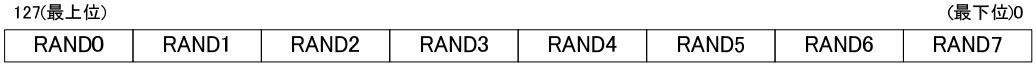
- ・AES5(AES_CTR_PIPE), AES12(JIP_PR_AESTOP), AES13(JIP_WO_AESTOP)にて IV として使用される.
- ・ASIC 回路の外部より 1 回でも IV データレジスタにデータを入力した場合, その次に行う暗号化処理において, IV が更新される.



③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データを保持する. 各暗号コアにより以下のように入力データサイズ, 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のこと.

・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
・MISTY1, T-DES, DES, CAST　64bit ブロック暗号群
　　ITEXT0-3　　64bit 入力
　　ITEXT4-31　　使用せず
・その他の暗号　　128bit ブロック暗号群
　　ITEXT0-7　　128bit 入力
　　ITEXT8-31　　使用せず

④乱数データレジスタ
・AES8(U_YNU_MA_AESTOP), AES9(U_YNU_ML_AESTOP), AES10 (U_YNU_TI_AESTOP) にて SEED として使用される.
・ASIC 回路の外部より 1 回でも乱数データレジスタにデータを入力した場合, その次に行う暗号化処理において, 乱数が更新される.
・AES9(U_YNU_ML_AESTOP)の乱数は, 32bit である. 乱数データレジスタの上位側につめて入力すること. (RAND0-1 に入力)




⑤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 の出力テキストデータを保持する. 各暗号コアにより以下のように出力データサイズ, データの出力される出力テキストレジスタの場所が異なるので注意のこと.

・AES5(AES_CTR_PIPE):　128bit×4 ブロック分出力される. (注)
　　OTEXT0-7　　128bit　1 ブロック目出力
　　OTEXT8-15　　128bit　2 ブロック目出力
　　OTEXT16-23　　128bit　3 ブロック目出力
　　OTEXT24-31　　128bit　4 ブロック目出力
・MISTY1, T-DES, DES, CAST　64bit ブロック暗号群
　　OTXT0-3　　64bit 入力
　　OTEXT4-7　　0x0000000000000000
　　OTXT8-31　　Don't care
・その他の暗号　128bit ブロック暗号群
　　OTEXT0-7　　128bit 出力
　　OTEXT8-31　　Don't care

(注)

・他の暗号コアと異なり連続データ入力(128bit×4 ブロック)＆連続データ出力(128bit×4 ブロック)で処理が行われる.

・ASIC 回路の外部より 1 回でも IV データレジスタにデータを入力した場合, その次に行う暗号化処理は, IV の設定動作が行われ, カウンターモードの乱数生成部分の処理のみが行われる. よって, 出力テキストレジスタ(OTEXT)には何もデータは出力されない. その次に行う暗号化処理にて, 入力テキストレジスタ(ITEXT)を使用した暗号化処理とその次の処理で使用される乱数生成部分の処理が行われる.

127(最上位)　　(最下位)0

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| OTEXT0 | OTEXT1 | OTEXT2 | OTEXT3 | OTEXT4 | OTEXT5 | OTEXT6 | OTEXT7 |
| OTEXT8 | OTEXT9 | OTEXT10 | OTEXT11 | OTEXT12 | OTEXT13 | OTEXT14 | OTEXT15 |
| OTEXT16 | OTEXT17 | OTEXT18 | OTEXT19 | OTEXT20 | OTEXT21 | OTEXT22 | OTEXT23 |
| OTEXT24 | OTEXT25 | OTEXT26 | OTEXT27 | OTEXT28 | OTEXT29 | OTEXT30 | OTEXT31 |

⑥中間値レジスタ:RDATA0-7

IP 選択レジスタ:IPSEL/OUTSEL で AES6 を選び, 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レジスタ. AES6 実行時の各ラウンドの中間値データの読み出しのためのレジスタ群である. 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.

・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, データの配列は RTEXT0 に最上位 16 ビット分のデータ, 以下 RTEXT1, RTEXT2…と続く.

・Fault Error 発生時

Fault Error が発生した際(AES_FA の Err[0]がアサート)には, 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.

なお, 中間値出力機能を使った場合でも AES6 の処理は最後まで継続し, 出力テキストデータが OTEXT に保持される.

127(最上位)　　(最下位)0

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| RTEXT0 | RTEXT1 | RTEXT2 | RTEXT3 | RTEXT4 | RTEXT5 | RTEXT6 | RTEXT7 |

⑦中間鍵レジスタ:RKEY0-7

IP 選択レジスタ:IPSEL/OUTSEL で AES6 を選び, 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レジスタ. AES6 実行時の各ラウンドの中間鍵データの読み出しのためのレジスタ群である. 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.

・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[KRSEL]で示されるラウンドの中間鍵が保持され, データの配列は RKEY0 に最上位 16 ビット分のデータ, 以下 RKEY1, RKEY2…と続く.

・Fault Error 発生時

Fault Error が発生した際(AES_FA の Err[1]がアサート)には, ラウンド選択レジスタ RSEL の KERR 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.

127(最上位) (最下位)0

| RKEY0 | RKEY1 | RKEY2 | RKEY3 | RKEY4 | RKEY5 | RKEY6 | RKEY7 |
|---|---|---|---|---|---|---|---|

### 3.5.3. 公開鍵暗号用レジスタ群

①指数レジスタ：EXP00-EXP1F

RSA： 512 ビットの指数データを入力する. EXP00 に最上位 16 ビット分の指数が保持され, 以下 EXP01, EXP02, …と続く.

ECC： 以下のデータを入力する.

EXP00-EXP03： 64 ビット秘密鍵データ

EXP04-EXP07： 64 ビット乱数データ

EXP08-EXP1F： 未使用

添字が若い側に上位のデータを入力する.

②法レジスタ：MOD00-MOD1F

RSA： 512 ビットの法データを入力する. MOD00 に最上位 16 ビット分の法が保持され, 以下 MOD01, MOD02, …と続く.

ECC： 以下のデータを入力する.

MOD00-MOD0B： 入力点の Affine 座標における x 座標データ(192 ビット)

MOD0C-MOD1F： 未使用

添字が若い側に上位のデータを入力する.

③前処理演算結果レジスタ：PREDAT00-PREDAT0F

RSA： CRT 処理時の 256 ビットの前処理演算結果のデータを入力する. PREDAT00 に最上位 16 ビットの前処理演算結果データが保持され, 以下 PREDAT01, PREDAT02, …と続く.

ECC：以下のデータを入力する.

PREDAT00-PREDAT0B：入力点の射影座標における Z 座標データ(192 ビット)

PREDAT0C-PREDAT0F：未使用

添字が若い側に上位のデータを入力する.

④入力データレジスタ：IDATA00-1F

RSA：512 ビットの入力データレジスタ. IDATA00 に最上位 16 ビットの入力データが保持され, 以下 IDATA01, IDATA02, …と続く.

ECC：以下のデータを入力する.

IDATA00-IDATA0B：楕円パラメータ b(192 ビット)

IDATA0C-IDATA1F:未使用

添字が若い側に上位のデータを入力する.

### 3.5.4. チップ情報レジスタ群

①バージョンレジスタ：VER

チップのバージョンを表す読み出し専用レジスタ．0xE27C が読みだされる．

## 3.6. 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に暗号LSIのクロック系統図を示す．

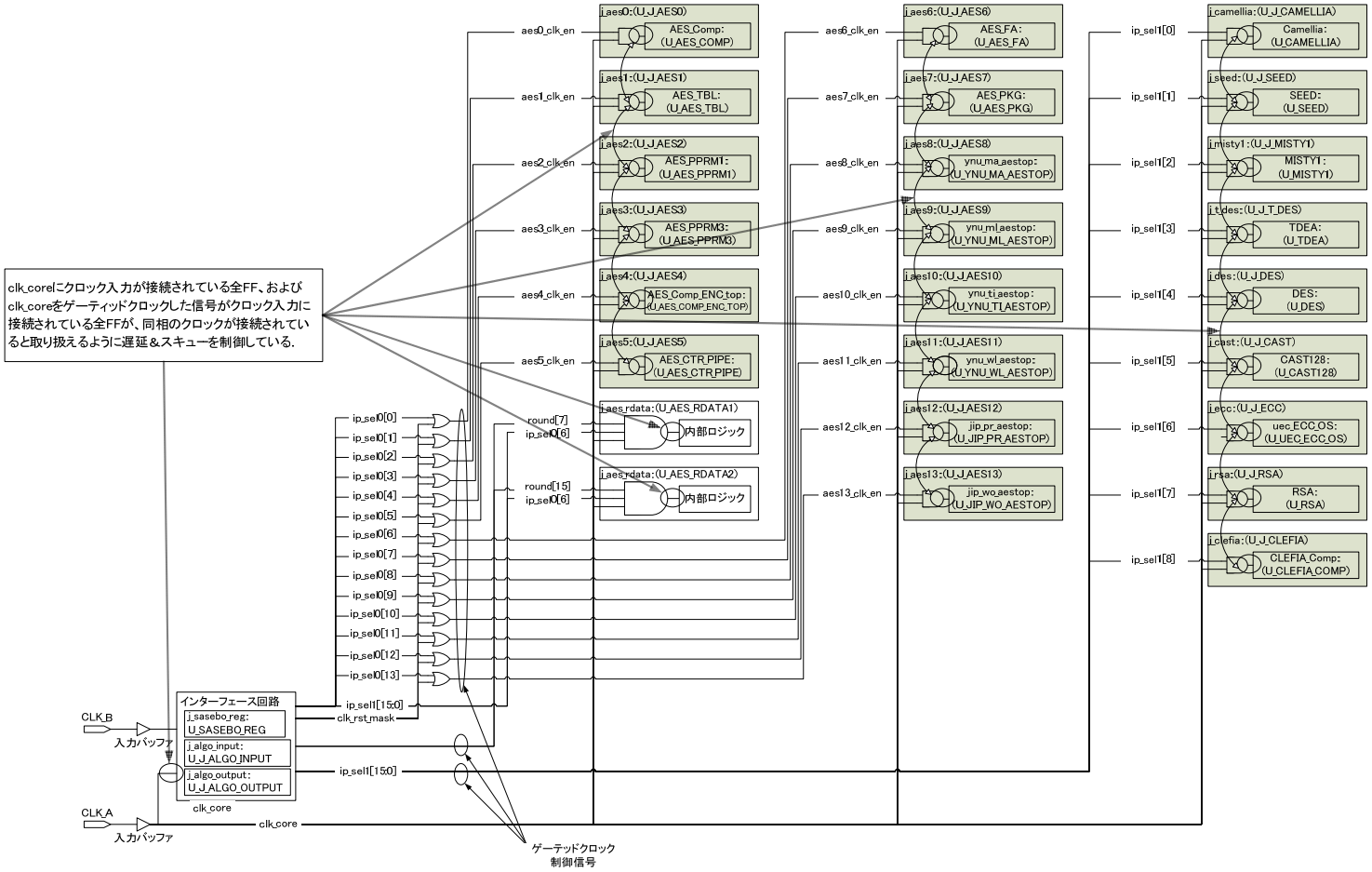



図 3-5　クロック系統図

## 3.7. リセット

本節では暗号LSIのリセットについて説明する. 図 3-6は暗号LSIのリセット系統である.
暗号 LSI のリセットシーケンスは以下となる.

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 のリセット信号は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になる. この時点では, 各コアにクロックは供給されておらず, 各コアへのリセット信号もアサートされたままである.

③ コア選択
インタフェース回路の IP 選択レジスタ:IPSEL0, 1 中の該当ビットをセットし, 動作させるコアを選択する. IPSEL0, 1 で選択されたコアに対してクロックが供給される. この時点では, 選択されたコアを含め, 各コアへのリセット信号はアサートされたままである.

④ 選択したコアのリセット解除
インタフェース回路のコントロールレジスタ:CONT 中の IPRST ビットに 0 を書き込むことで, ③で選択したコアのリセット信号がデアサートされ, リセットが解除される. なお, リセットシーケンスには関係ないが, 暗号 LSI の動作手順としては, このあと出力選択レジスタ: OUTSEL0, 1 の設定を行う.

また, IP 選択レジスタで選択されていないコアについては, クロックも供給されず, リセット信号もアサートされたままである点に留意こと.

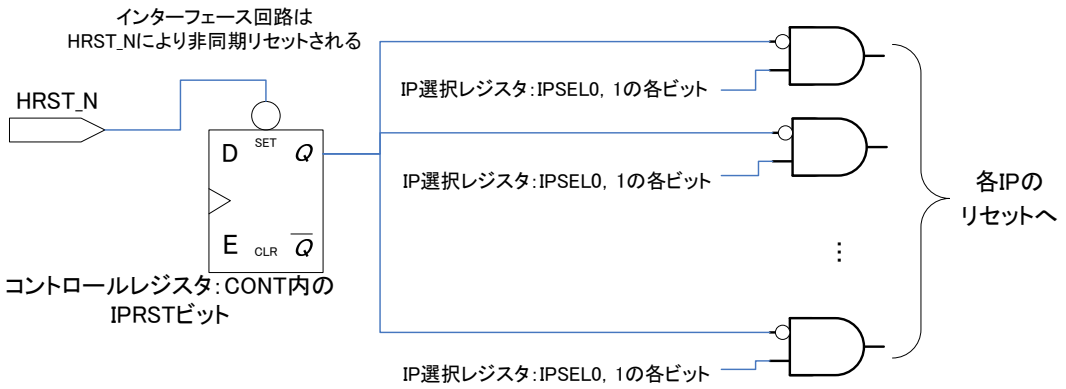



図 3-6　リセット系統

## 3.8. 付帯機能および留意事項

本節ではこれまで取り上げられなかった各種の付帯機能および留意点について説明する.

### 3.8.1. コアクロックとインタフェースクロックについて

故障解析を容易にすることを狙って，コアのみに動作クロック由来の故障を印加するため，コアクロックとインタフェースクロックを分離している．この影響で，暗号 LSI 内同期化回路の簡略化のため，インタフェースクロック周波数＜コアクロック周波数，ということを前提に設計を行っている．つまり，暗号 LSI に供給するクロックは，

CLK_A 周波数＞CLK_B 周波数

である必要がある．(CLK_A が 24MH z であれば CLK_B は 23MH z 程度で構わない．基板上で煩雑になるようであれば, 単純に CLK_A を 2 分周して CLK_B を 12MH z としても構わない．)

### 3.8.2. 鍵長制限

暗号 LSI の設計データ(RTL)には，LSI の輸出管理対策として，アルゴリズムコアの鍵長を制限するための記述を付加している．このため，共通鍵アルゴリズムは 56 ビットに鍵長が制限される.(RSA と ECC はコア自身がそれぞれ 512 ビット, 64 ビットに制限している.) 各共通鍵アルゴリズムコアの鍵の取扱いは以下の通り.

(1) DES：パリティビットを含まない 56bit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 3-7に示す.

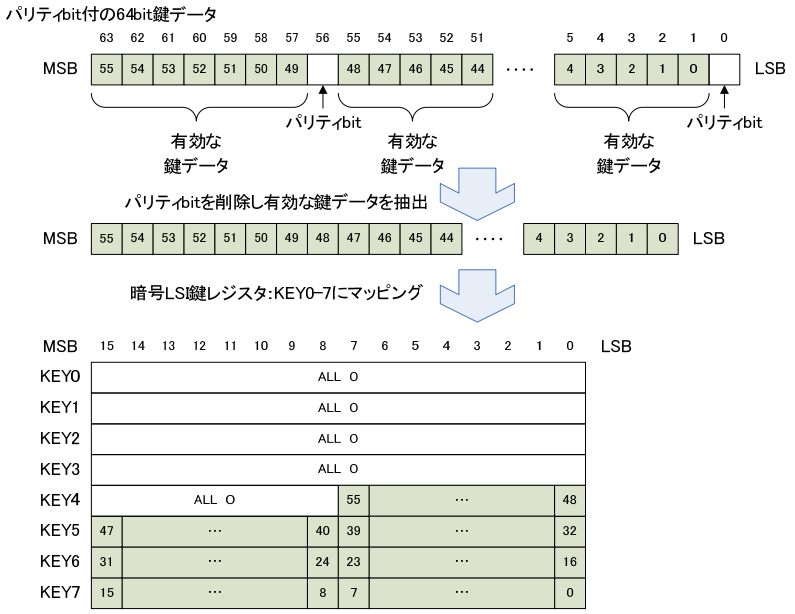



図 3-7　DES 鍵データビットアサイン

(2) T-DES：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 同じである．

[191:64]：　0x000102030405060708090a0b0c0d0e0f (固定値)

(3) その他共通鍵暗号：コアの鍵長が 128 ビットであり，以下のような取扱いとしている．

[127：56]：　0x000102030405060708 (固定値)

[55:0]：　外部より入力される鍵 KEY4 下位 8 ビットと KEY5-7 を併せた 56 ビット

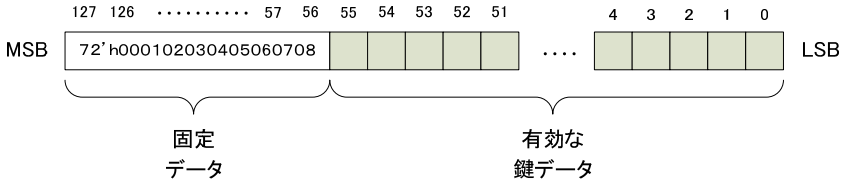



図 3-8　鍵データビットアサイン

### 3.8.3. 遅延実行

暗号 LSI では鍵設定やデータ入出力による電力の変動と，実際の暗号処理の電力を時間的に分離することにより，より精度よく電力波形を観測できるように工夫している．

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後に評価用信号(START_N，EXEC)をアサート，更に 8 CLK後に暗号アルゴリズムコアに対して処理開始信号をアサートする．(CLKはいずれもCLK_A換算) アルゴリズムコアの処理終了時は，コアの演算終了信号アサート後，8CLK後に評価用信号END_Nアサート/EXECでアサート，更に 8CLK後にコントロールレジスタCONT[RUN]を 0 にする．詳しい動作の様子を図 3-9に示す．

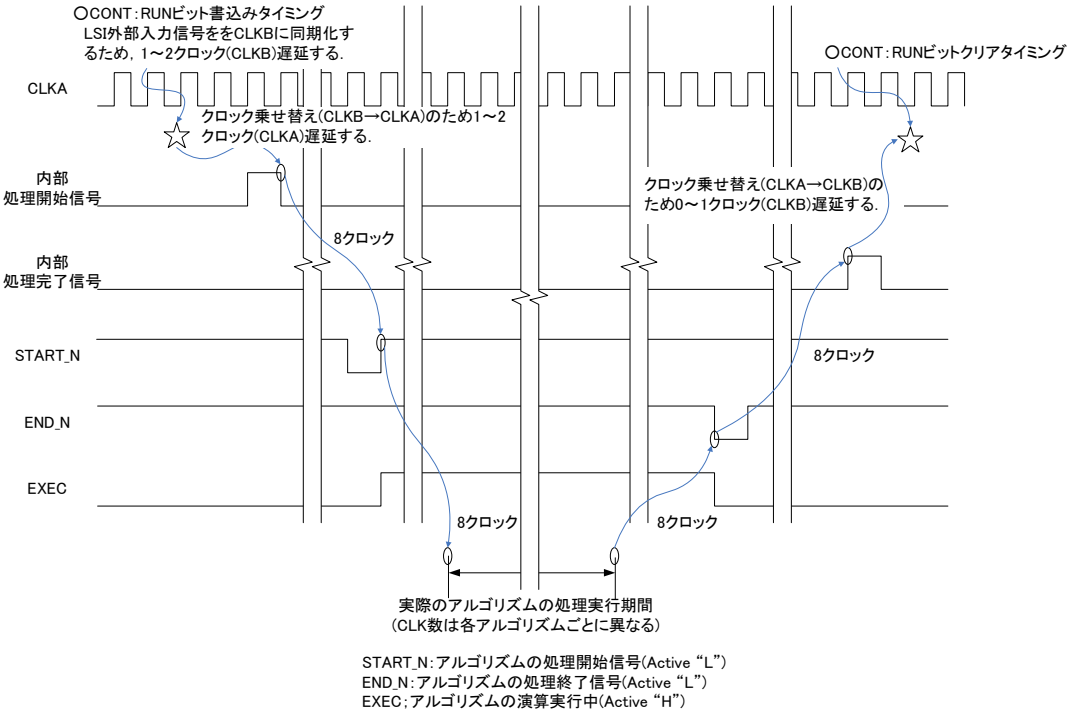



図 3-9　遅延実行タイミングチャート

### 3.8.4. ノイズ源

将来的に，対象とする暗号アルゴリズムコア以外の電力，つまりノイズ成分が電力解析や電磁波解析に与える影響を評価できるように，評価対象以外の暗号アルゴリズムコアをノイズ発生源として利用できる構成としている．具体的には，IP 選択レジスタ：IPSEL で複数の暗号アルゴリズムコアを選択し，出力選択レジスタ：OUTSEL で評価対象の暗号コアのみを選択することにより，評価対象以外の暗号アルゴリズムコアをノイズ源として使用可能な構成としている．

### 3.8.5. 自走モード

コントロールレジスタ CONT[RUN]を 1 にすると 0.3 秒ごとに自動的に暗号化処理を続ける動作モードである．詳細は、以下の通り．

- AES0(AES_Comp)のみでサポート
- 1 回目の暗号化処理が終了すると，コントロールレジスタ CONT[RUN]は 0 のままとなり、2 回目以降の暗号化処理時に 1 にはならない．
- 出力抑止機能を使用していない限り，START_N，EXEC，END_N は上記の遅延実行で記述している様に制御される。
- 自走モード動作中に，他の処理を実行させる事は禁止である．また、自走モードを解除するには，PowerOFF もしくは HRST_N をアサートする必要がある．
- 以下の 2 つの自走モードをサポートする
  ① 入力テキストレジスタ(ITEXT)のデータを初期値として, +1 インクリメントしながら自走する．(モードレジスタ MODE[FRUN]を 2’b10 に設定)
  ② 入力テキストレジスタ(ITEXT)のデータを初期値として，暗号化(復号)結果を次回の入力にしながら自走する. (モードレジスタ MODE[FRUN]を 2’b11 に設定)

### 3.8.6. 評価用信号の出力抑止機能

評価用信号からのノイズ放射を低減するため，START_N，END_N，EXEC，STATE の出力を抑止する機能を設けている．出力抑止機能は，START_N，END_N，EXEC をデアサート状態，STATE を 0 固定とする．以下の 2 つのモードをサポートする．

① 全評価用信号の出力抑止：モードレジスタ MODE[OUTINH]を 2’b10 に設定
② START_N 以外の出力抑止：モードレジスタ MODE[OUTINH]を 2’b11 に設定

### 3.8.7. 入力テキストレジスタ(ITEXT)の取扱い

共通鍵暗号アルゴリズムコアでは各コアで以下のように入力データサイズ，入力テキストレジスタのマッピングが異なるので留意のこと．

①AES5(CTR モードサポートパイプライン実装)
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 |

②MISTY1，T-DES，DES，CAST-128(64bit ブロック暗号)

| | |
|---|---|
| ITEXT0-3 | 64bit 入力 |
| ITEXT4-31 | 未使用 |

③その他の暗号(128bit ブロック暗号)

ITEXT0-7　　128bit 入力
ITEXT8-31　 未使用

### 3.8.8. 出力テキストレジスタ(OTEXT)の取扱い

共通鍵暗号アルゴリズムコアでは各コアで以下のように出力データサイズ，出力テキストレジスタのマッピングが異なるので留意のこと．

①AES5(CTR モードサポートパイプライン実装)

128bit×4 ブロック出力される．

OTEXT0-7　　128bit　1 ブロック目出力
OTEXT8-15　 128bit　2 ブロック目出力
OTEXT16-23　128bit　3 ブロック目出力
OTEXT24-31　128bit　4 ブロック目出力

②MISTY1，T-DES，DES，CAST-128(64bit ブロック暗号)

OTEXT0-3　　64bit 出力
OTEXT4-7　　0x0000000000000000
OTEXT8-1F　 don't care

③その他の暗号(128bit ブロック暗号)

OTEXT0-7　　128bit 出力
OTEXT8-1F　 don't care

### 3.8.9. DPA対策用の乱数(SEED)レジスタ(RAND)の取扱い

・AES8 (Masked AND Operation), AES9(MDPL), AES10(Threshold Implementation)で使用される．
・暗号 LSI 外部より乱数データレジスタに SEED データを入力すると、その次の暗号化で SEED を反映した処理を実行する．
・AES9(MDPL)で使用される乱数 SEED は 32bit である．乱数データレジスタの上位側が有効となる．(RAND0-1 に入力)

### 3.8.10. 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連続データ入力(128bit×4 ブロック)&連続データ出力(128bit×4 ブロック)で処理が行われる．
・暗号 LSI 外部から IV データレジスタにカウンタ初期値データを入力して暗号化処理を行なうと、直後の処理ではカウンターモードの乱数生成部分の処理のみが行われるため，出力テキストレジスタ(OTEXT)には暗号化データが出力されない。その次に行う暗号化処理で，入力テキストレジスタ(ITEXT)を暗号化したデータの出力と，その次の 4 ブロックの乱数生成が行われる。

### 3.8.11. 中間値データの出力

暗号アルゴリズムの演算途中の値を出力させる機能．詳細は以下．

・AES6(故障攻撃耐性評価用実装)のみでサポートする．IP 選択レジスタ(IPSEL0)及び出力選択レジスタ(OUTSEL0)で AES6 が選択されていて，ラウンド選択レジスタ DRSEL[DEN]が 1 の時に中間値データレジスタ(RDATA0-7)に中間値が出力される．
・出力される中間値データの場所は、ラウンド選択レジスタ DRSEL[DRSEL]の値で決定する．
・中間値データは AES6 の出力 Dout から取得している．

### 3.8.12. 中間鍵データの出力

暗号アルゴリズムの演算最中の鍵を出力させる機能．詳細は以下.

・AES6(故障攻撃耐性評価用実装)のみでサポートする. IP 選択レジスタ(IPSEL0)及び出力選択レジスタ(OUTSEL0)で AES6 が選択されていて，ラウンド選択レジスタ KRSEL[KEN]が 1 の時に中間鍵レジスタ(RKEY0-7)に中間鍵データが出力される.

・出力される中間鍵データの場所は, ラウンド選択レジスタ KRSEL[KRSEL]の値で決定する.

・中間鍵データは AES6 の Kout 出力から取得している。

### 3.8.13. FA(Fault Attack)対策機能への対応

暗号アルゴリズムの演算最中に Fault Error が起きた場合の処理である．Fault Attack 対策機能が実装されている AES6(故障攻撃耐性評価用実装)のみでサポートする．AES6 内で，Fault Error が起きた場合には，ラウンド選択レジスタの KRSEL[KERR]あるいは DRSEL[DERR]が 1 となり，その時の出力データの値と鍵の値がそれぞれ中間値レジスタ(RDATA0-7)及び中間鍵レジスタ(RKEY0-7)に出力される.

### 3.8.14. 暗号アルゴリズム演算中のインタフェース回路の挙動について

よりノイズを削減し高精度な測定を行なうため，図 3-10に示すように暗号アルゴリズムの演算中にインタフェース回路が動作しないよう改善を行なった.

なお, 平成 20 年度開発の暗号 LSI については以下の操作を暗号化スタート前に行うことにで，同様の効果を得ることができる.

① 鍵データを鍵レジスタに Write する.

② CONT レジスタの KSET に"1"を Write する.

→鍵データが暗号 IP に転送され，鍵生成処理を行なう.

③ その後，鍵レジスタに ALL"0"を Write する.

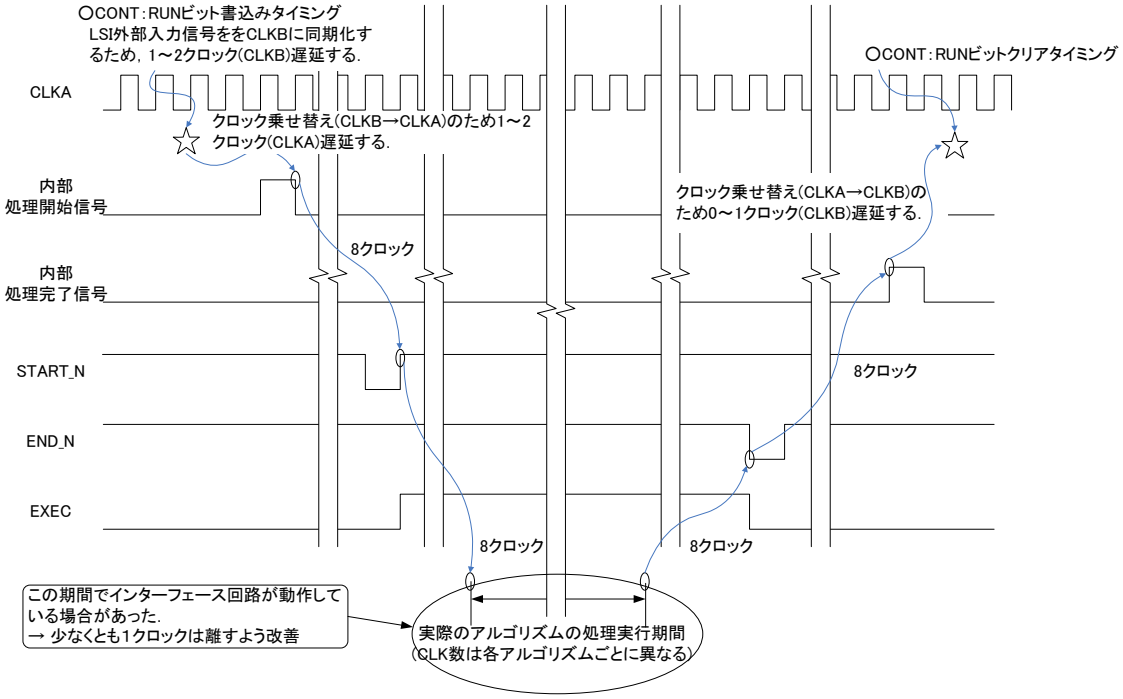



図 3-10　インタフェース動作期間の改善

# 4. 論理シミュレーションによる動作検証用環境

## 4.1. 動作検証用モジュール概要

動作検証用モジュールは，評価用 LSI 全体の RTL を論理シミュレータ上で動作させるための入力信号供給，及び LSI 出力値を予め用意した出力期待値と照合し評価用 LSI 全体の動作を検証するためのモジュールである．動作検証モジュールは，評価用 LSI 全体の RTL と同じく，ハードウェア記述言語で記述され，評価用 LSI の RTL と共に論理シミュレータ上でシミュレーションを実行する．

## 4.2. 動作検証モジュールの機能

動作検証モジュールが供給する評価用 LSI に対する入力信号は，各暗号コアアルゴリズムのテストベンチ(各暗号アルゴリズムコアの動作検証モジュール)で使用しているテストベクタをベースに作成されている．各暗号アルゴリズムコアのテストベンチから鍵データ及び入力文データを抽出し，2 章で示した外部仕様に基づく入力信号を供給することにより評価用 LSI の RTL を動作させる。

一方，同じく各暗号アルゴリズムコアのテストベンチから出力期待値を抽出し，RTL の出力と照合することにより，評価用 LSI の論理動作の検証を行う．

## 4.3. 動作検証モジュールを用いた検証および検証結果

検証する項目及び検証結果を表 4-1および表 4-2に示す．

表 4-1　検証項目及び検証結果(1/2)

| 暗号アルゴリズムコア | 検証項目 | 確認データ(数) | 検証結果 |
|---|---|---|---|
| AES0 | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| AES1 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES2 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES3 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES4 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES5 | | 8 ブロック | ○ |
| AES6 | 暗号化 | 1 ブロック | ○ |
| | 暗号化時<br>中間値出力 | 0 ラウンド(KEY との EXOR のみ)～20 ラウンド目までの各中間値出力 | ○ |
| | 暗号化時<br>中間鍵出力 | 0 ラウンド(KEY との EXOR のみ)～20 ラウンド目までの各中間値出力 | ○ |
| | 暗号化時<br>Fault 攻撃 | 中間値レジスタ、中間鍵レジスタへの出力 | ○ |
| | 復号 | 1 ブロック | ○ |
| | 復号時<br>中間値出力 | 0 ラウンド(KEY との EXOR のみ)～20 ラウンド目までの各中間値出力 | ○ |
| | 復号時中間<br>値出力 | 0 ラウンド(KEY との EXOR のみ)～20 ラウンド目までの各中間値出力 | ○ |
| | 復号時<br>Fault 攻撃 | 中間値レジスタ、中間鍵レジスタへの出力 | ○ |
| AES7 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES8 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES9 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES10 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES11 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES12 | 暗号化 | 同一データで 2 ブロック | ○ |
| AES13 | 暗号化 | 同一データで 2 ブロック | ○ |

表 4-2　検証項目及び検証結果(2/2)

| 暗号アルゴリズム コア | 検証項目 | 確認データ(数) | 検証結果 |
|---|---|---|---|
| Camellia | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| SEED | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| MISTY1 | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| T-DES (Triple-DES) | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| DES | 暗号化 | 3 ブロック | ○ |
| | 復号 | 3 ブロック | ○ |
| CAST-128 | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| CLEFIA | 暗号化 | 1 ブロック | ○ |
| | 復号 | 1 ブロック | ○ |
| ECC | 演算 | 100 ブロック | ○ |
| RSA | べき乗 剰余演算 (通常モード) | 6 通りの全ての演算手法で 512bit 1 回 | ○ |
| | べき乗 剰余演算 (CRT モード) | 6 通りの全ての演算手法で 512bit(256bit×2)を 1 回 | ○ |

# 5. 論理合成制約について

評価用 LSI の RTL は，次の点に留意して論理合成以降の作業を実施する必要がある．

「ゲーティッドクロックに配慮した CTS(Clock Tree Synthesis)及びクロックスキュー制御」

評価用 LSI 内のクロックのうち暗号アルゴリズムコアを動作させる CLK_A(コアクロック)を使用したクロックはすべて、1 相同期クロックであることを前提に設計している．このため，IP 選択レジスタにより供給/停止が制御される各暗号アルゴリズムコアのクロック 23 系統，AES6 中間値出力制御回路用のクロック 1 系統，AES6 中間鍵出力制御回路用のクロック 1 系統，及び常時供給されるインタフェースクロック CLK_B との乗せ変え部分のクロック 1 系統の全てを同一のクロックラインとして取り扱えるよう，CTS 及びクロックスキューの制御を論理合成/配置配線工程で実施する。

クロック系統に関しては，図 3-5を参照のこと。

# 6. LSIの物理レイアウト

## 6.1. 設計環境

今回作成した暗号LSIは，2.1×2.1mm$^2$ のダイサイズのうち 77.72%のゲートが使用されている．目標動作周波数は 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．暗号LSIの概要を表 6-1に示す．使用したテクノロジは富士通CS202L (65mn)であり，ライブラリは株式会社イーシャトルのもである．使用ライブラリの詳細を表 6-2に，論理合成条件を表 6-3に示す．

表 6-1　暗号 LSI の概要

| 項目 | |
|---|---|
| ライブラリ | 富士通 イーシャトル CS202 (LVt) |
| プロセス | 65nm CMOS |
| 置配線層 | メタル 12 層 |
| ダイサイズ | 2.1mm × 2.1mm |
| パッケージ | セラミック QFP 160 pin |
| セル面積 | 1,404,242 um$^2$ |
| ゲート数 | 731,376　2-NAND gates |
| セル使用率 | 77.72% |
| 動作周波数 | 35.1MHz |

表 6-2　使用ライブラリ詳細

| 分類 | Library | プロセス |
|---|---|---|
| Standard Cell | CS202L CS202MZ(12 Tracks LVt) | CS202L |
| Digital I/O | CS202L Common | CS202L |
| RAM | ChaRAM | CS202L |

表 6-3　論理合成条件

| 条件項目 | | 条件値 |
|---|---|---|
| 設定周波数 | CLKA | 31MHz　(32000 ps)　+30%マージン含む |
| | CLKB | 31MHz　(32000 ps)　+30%マージン含む |
| 入出力遅延 | 入力遅延 | 2000 ps |
| | 出力遅延 | 2000 ps |
| 仮負荷制約 | | cs202mx_3600area |

## 6.2. 論理合成結果

論理合成の結果得られた面積を表 6-4に，消費電力の概算を表 6-5に示す．

表 6-4　面積レポート

| 階層名 | セル面積[um$^2$] | セル面積<br>[2 入力 NAND 換算※] | 割合[%] | インスタンス数 |
|---|---|---|---|---|
| J_SASEBO_ASIC_TOP | 1,387,994 | 722,914 | 100 | 269,562 |
| U_AES_RDATA1 | 1,928 | 1,004 | 0.1 | 161 |
| U_AES_RDATA2 | 1,928 | 1,004 | 0.1 | 161 |
| U_J_AES0 | 42,104 | 21,929 | 3 | 10,349 |
| U_J_AES1 | 34,969 | 18,213 | 2.5 | 11,618 |
| U_J_AES2 | 95,268 | 49,619 | 6.9 | 28,435 |
| U_J_AES3 | 25,500 | 13,281 | 1.8 | 6,565 |
| U_J_AES4 | 20,007 | 10,421 | 1.4 | 4,975 |
| U_J_AES5 | 39,274 | 20,455 | 2.8 | 7,178 |
| U_J_AES6 | 32,041 | 16,688 | 2.3 | 7,601 |
| U_J_AES7 | 37,295 | 19,424 | 2.7 | 4,827 |
| U_J_AES8 | 72,646 | 37,836 | 5.2 | 13,220 |
| U_J_AES9 | 127,345 | 66,326 | 9.2 | 27,810 |
| U_J_AES10 | 207,247 | 107,941 | 14.9 | 30,477 |
| U_J_AES11 | 56,056 | 29,196 | 4 | 11,610 |
| U_J_AES12 | 61,210 | 31,880 | 4.4 | 10,842 |
| U_J_AES13 | 38,101 | 19,845 | 2.7 | 5,717 |
| U_J_CAMELLIA | 23,230 | 12,099 | 1.7 | 6,627 |
| U_J_SEED | 33,951 | 17,683 | 2.4 | 10,893 |
| U_J_MISTY1 | 27,338 | 14,239 | 2 | 8,774 |
| U_J_T_DES | 8,763 | 4,564 | 0.6 | 2,066 |
| U_J_DES | 5,501 | 2,865 | 0.4 | 1,497 |
| U_J_CAST | 46,095 | 24,008 | 3.3 | 13,118 |
| U_J_ECC | 138,838 | 72,311 | 10 | 16,984 |
| U_J_RSA | 106,884 | 55,669 | 7.7 | 16,692 |
| U_J_CLEFIA | 15,576 | 8,113 | 1.1 | 3,521 |

表 6-5　消費電力概算レポート

| 階層名 | Switching Power[W] | Internal Power[W] | Leak Power[pW] | Total Power[W] | Percentage[%] |
|---|---|---|---|---|---|
| J_SASEBO_ASIC_TOP | 2.69E-04 | 1.04E-03 | 2.94E+10 | 3.07E-02 | 100 |
| U_AES_RDATA2 | 3.69E-09 | 7.19E-09 | 4.49E+07 | 4.49E-05 | 0.1 |
| U_AES_RDATA1 | 3.69E-09 | 7.19E-09 | 4.49E+07 | 4.49E-05 | 0.1 |
| U_J_AES0 | 2.32E-08 | 1.00E-07 | 7.47E+08 | 7.47E-04 | 2.4 |
| U_J_AES1 | 1.37E-08 | 5.10E-08 | 6.24E+08 | 6.25E-04 | 2 |
| U_J_AES2 | 1.49E-08 | 5.28E-08 | 1.42E+09 | 1.42E-03 | 4.6 |
| U_J_AES3 | 1.30E-08 | 5.12E-08 | 4.17E+08 | 4.17E-04 | 1.4 |
| U_J_AES4 | 1.30E-08 | 5.23E-08 | 3.45E+08 | 3.45E-04 | 1.1 |
| U_J_AES5 | 5.28E-06 | 1.70E-07 | 6.66E+08 | 6.72E-04 | 2.2 |
| U_J_AES6 | 9.23E-09 | 3.73E-08 | 5.57E+08 | 5.57E-04 | 1.8 |
| U_J_AES7 | 4.40E-05 | 3.02E-05 | 4.20E+08 | 4.94E-04 | 1.6 |
| U_J_AES8 | 1.24E-08 | 3.92E-08 | 2.59E+09 | 2.59E-03 | 8.5 |
| U_J_AES9 | 5.34E-06 | 8.15E-08 | 2.36E+09 | 2.37E-03 | 7.7 |
| U_J_AES10 | 5.29E-06 | 9.74E-08 | 7.39E+09 | 7.40E-03 | 24.1 |
| U_J_AES11 | 5.26E-06 | 6.62E-08 | 1.23E+09 | 1.23E-03 | 4 |
| U_J_AES12 | 1.31E-08 | 4.69E-08 | 2.00E+09 | 2.00E-03 | 6.5 |
| U_J_AES13 | 6.80E-09 | 3.35E-08 | 1.21E+09 | 1.21E-03 | 3.9 |
| U_J_CAMELLIA | 0 | 0 | 3.71E+08 | 3.71E-04 | 1.2 |
| U_J_SEED | 0 | 0 | 6.18E+08 | 6.18E-04 | 2 |
| U_J_MISTY1 | 0 | 0 | 4.75E+08 | 4.75E-04 | 1.5 |
| U_J_T_DES | 0 | 0 | 1.41E+08 | 1.41E-04 | 0.5 |
| U_J_DES | 0 | 0 | 8.86E+07 | 8.86E-05 | 0.3 |
| U_J_CAST | 0 | 0 | 1.06E+09 | 1.06E-03 | 3.4 |
| U_J_ECC | 1.40E-05 | 1.71E-05 | 1.87E+09 | 1.90E-03 | 6.2 |
| U_J_RSA | 0 | 0 | 1.76E+09 | 1.76E-03 | 5.7 |
| U_J_CLEFIA | 0 | 0 | 2.22E+08 | 2.22E-04 | 0.7 |

Switching Power　：ドライブセルの出力負荷容量によって発生する消費電力。
Internal Power：ドライブセルの入力変化によって生じる消費電力。
(貫通電流による消費電力含む)
Leak Power：動作待機時の消費電力。

## 6.3. 電源プラン

図 6-1は暗号LSIの電源ラインを除いたTop Viewを，図 6-2は電源ラインを示している．今回の暗号LSIでは，電源リング内部でストライプを張り，電源メッシュを作成した．電源メッシュは図 6-3 のようになっており，Metal4，Metal7，Metal9，およびMetal10 を使用して作成されている．スタンダードセルへの電源は，図 6-4 のように 4Metalのストライプからの Stack Viaによって供給している．各メッシュは電源リングに直接接続されており，IO-BUFの電源の引き込みにはMetal11，Metal12 を使用している(図 6-5)．

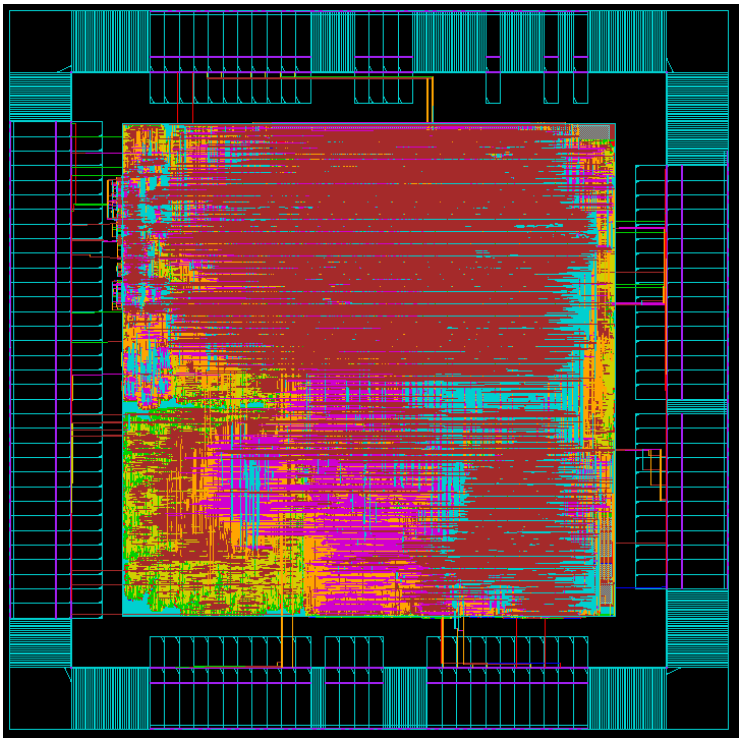



図 6-1　暗号 LSI のトップビュー

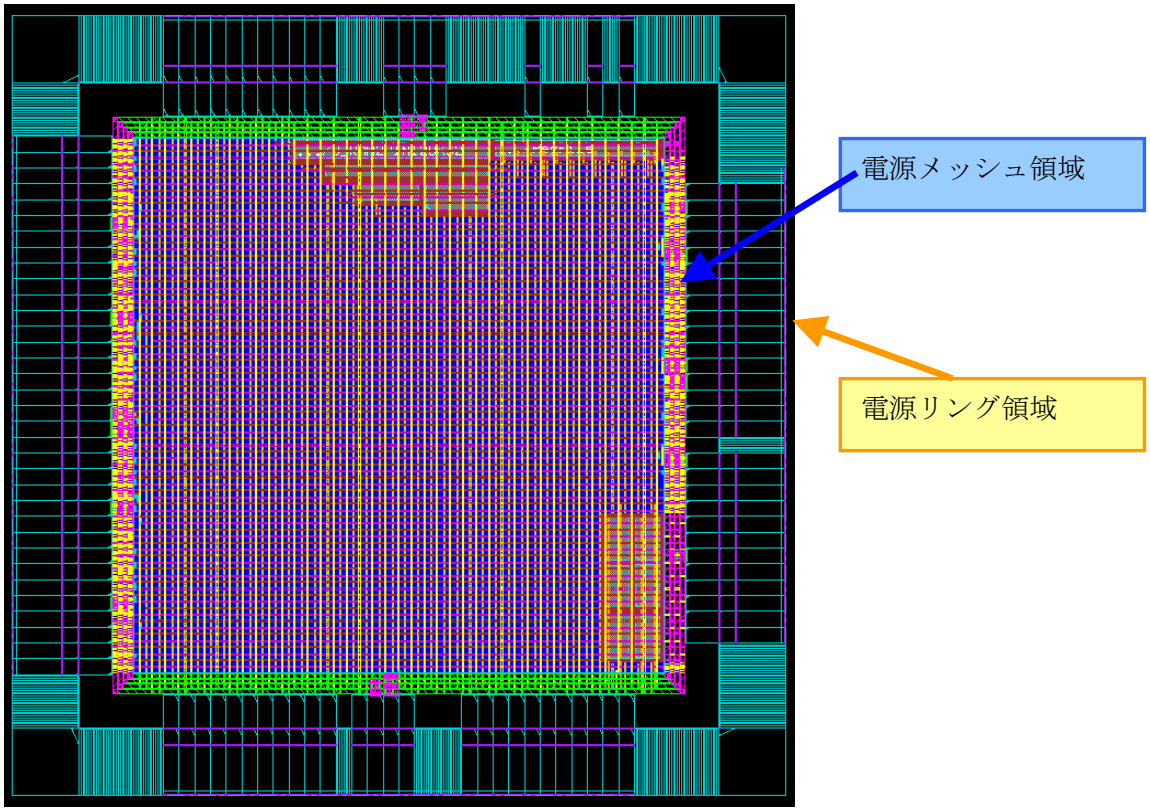



図 6-2　電源ライン

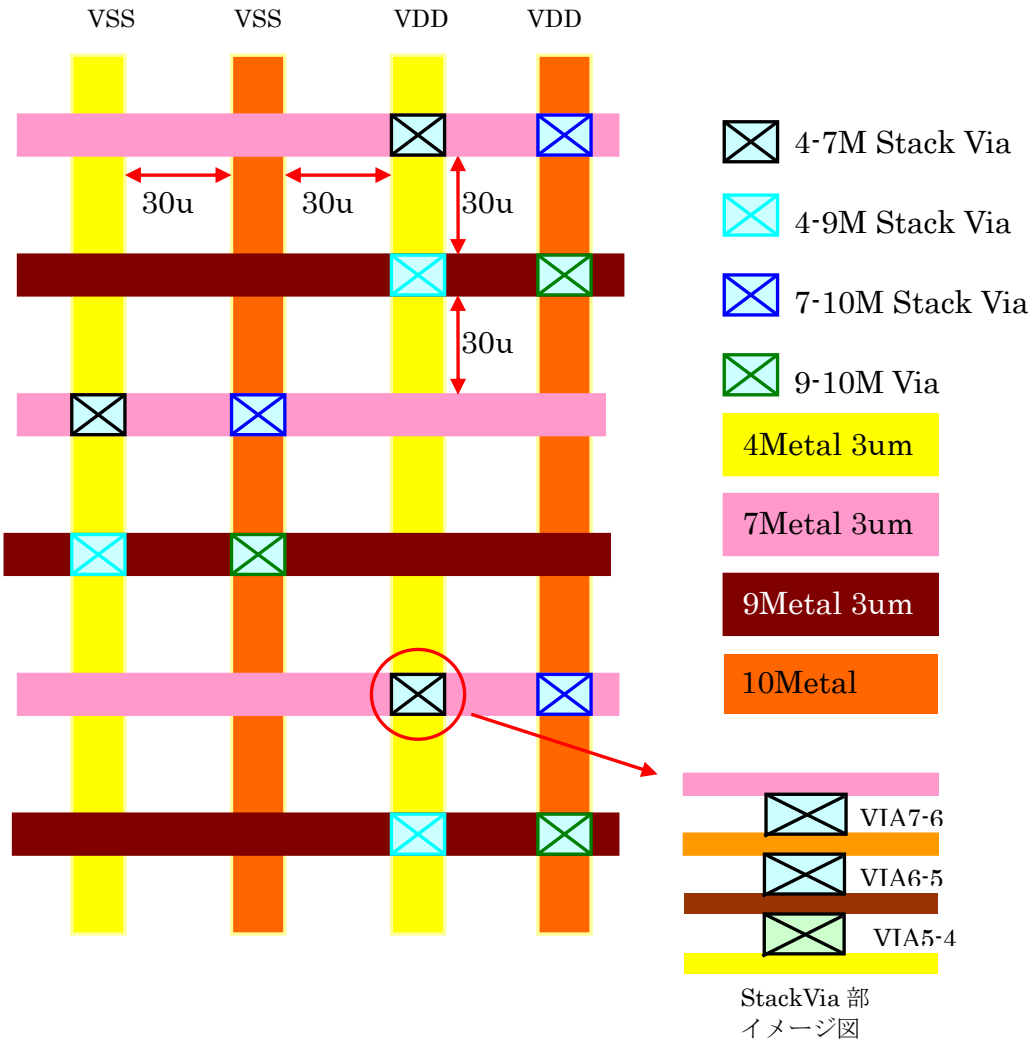



図 6-3　電源メッシュ

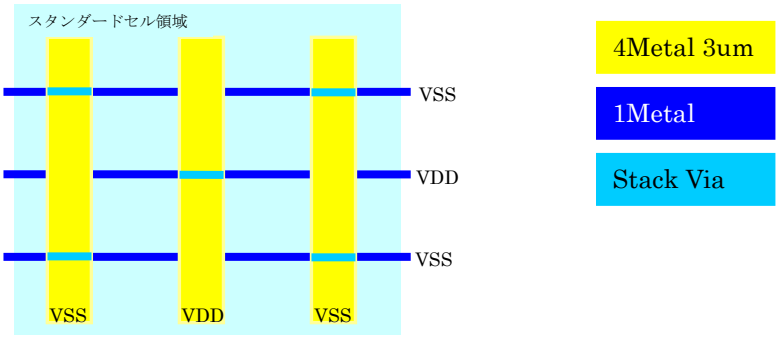



図 6-4　スタンダードセルへの電源供給

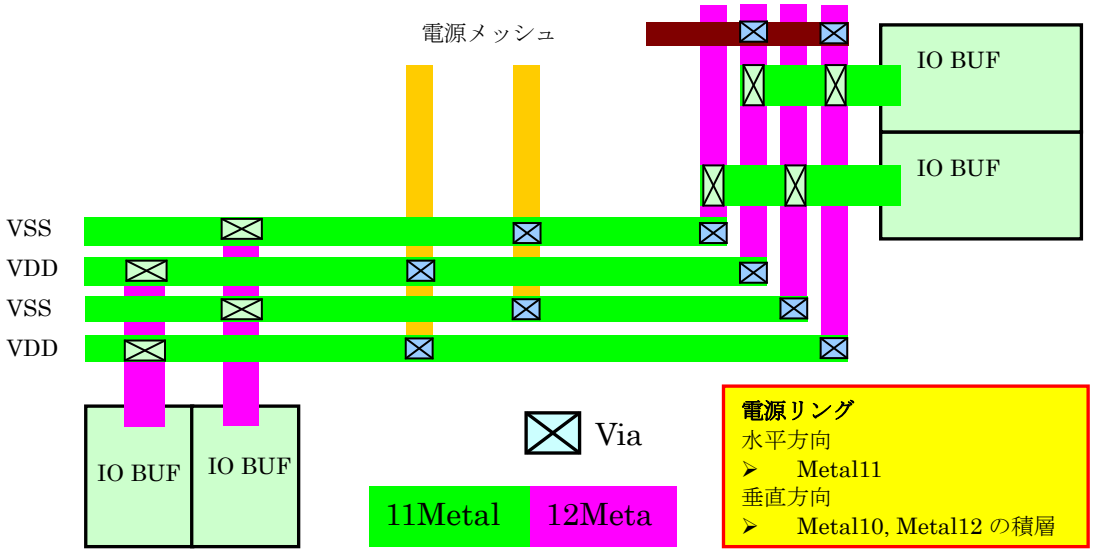



図 6-5　電源リング

## 6.4. マクロ配置

図 6-6にマクロの配置を示す.

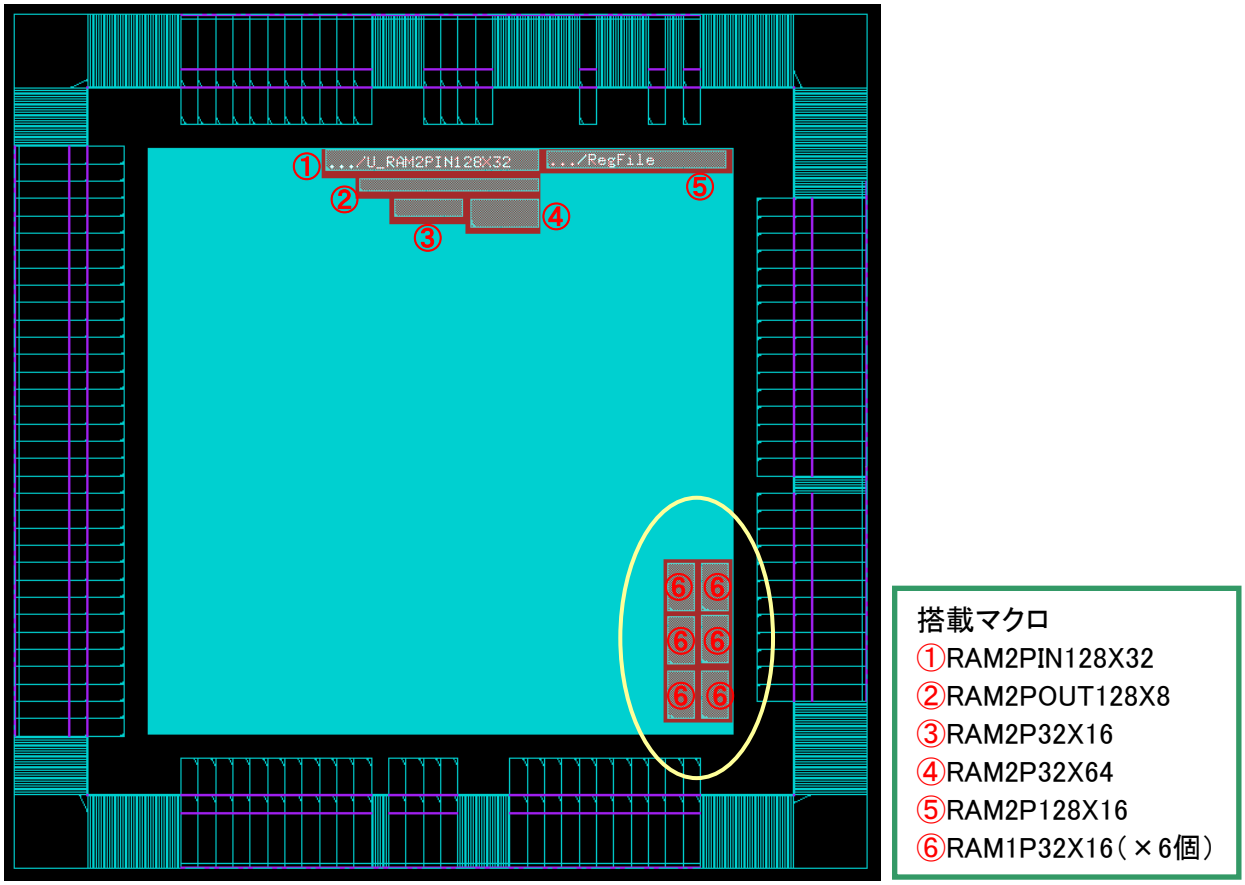



図 6-6　マクロの配置

## 6.5. モジュール配置

図 6-7に主なモジュールの配置を示す. これらのモジュールは初期配置の段階で配置領域指定を行い, 機能ごとに区分けしてレイアウトされるようにしている.

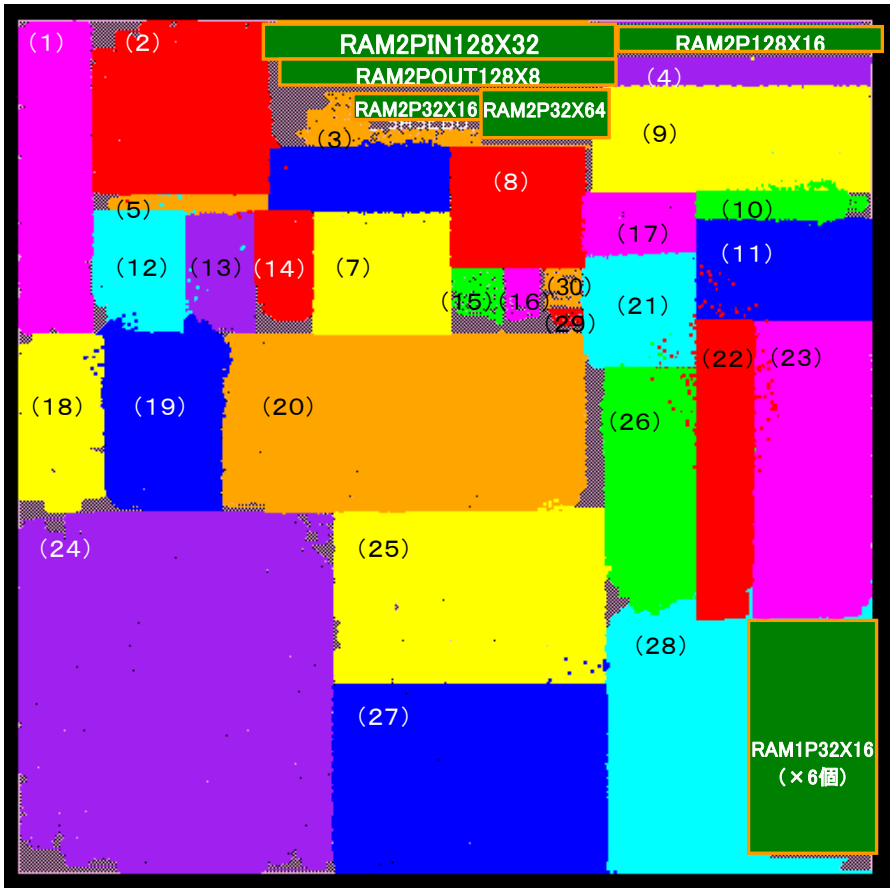



図 6-7　主なモジュールの配置

表 6-6　主なモジュール

| モジュール名 | 図番号 | セル面積 [um2] | インスタンス数 | モジュール名 | 図番号 | セル面積 [um$^2$] | インスタンス数 |
|---|---|---|---|---|---|---|---|
| U_J_AES0 | 26 | 45,344 | 11,098 | U_J_CAMELLIA | 6 | 24,927 | 7,257 |
| U_J_AES1 | 22 | 36,470 | 11,940 | U_J_SEED | 7 | 35,223 | 11,179 |
| U_J_AES2 | 25 | 97,306 | 28,814 | U_J_MISTY1 | 18 | 27,799 | 8,876 |
| U_J_AES3 | 21 | 27,110 | 6,895 | U_J_T_DES | 14 | 9,612 | 2,349 |
| U_J_AES4 | 12 | 21,852 | 5,324 | U_J_DES | 5 | 5,825 | 1,576 |
| U_J_AES5 | 19 | 46,213 | 8,732 | U_J_CAST | 1 | 46,993 | 13,239 |
| U_J_AES6 | 8 | 33,339 | 7,993 | U_J_ECC | 28 | 158,845 | 21,600 |
| U_J_AES7 | 4 | 38,663 | 5,047 | U_J_RSA | 27 | 114,815 | 18,517 |
| U_J_AES8 | 23 | 62,055 | 13,602 | U_J_CLEFIA | 13 | 17,364 | 4,097 |
| U_J_AES9 | 20 | 131,948 | 28,769 | U_AES_RDATA1 | 15 | 3,573 | 345 |
| U_J_AES10 | 24 | 171,577 | 30,930 | U_AES_RDATA2 | 16 | 3,320 | 356 |
| U_J_AES11 | 2 | 60,260 | 12,404 | U_SASEBO_VALUE | 29 | 269 | 68 |
| U_J_AES12 | 9 | 53,180 | 11,129 | U_SASEBO_ALGO_OUTPUT | 10 | 13,319 | 2,679 |
| U_J_AES13 | 11 | 33,927 | 6,083 | U_SASEBO_INPUT | 30 | 1,361 | 106 |
| U_SASEBO_REG | 3 | 75,072 | 926 | U_SASEBO_ALGO_INPUT | 17 | 20,565 | 5,638 |

## 6.6. セル面積レポート

最終ネットリストを使用し，Design Compilerを用いてレイアウトを行った．レイアウト後の面積レポートを表 6-7に，レイアウト前後での面積比較を表 6-8に示す．

表 6-7　レイアウト後の面積レポート

| 階層名 | セル面積［um²］ | セル面積 [2 入力 NAND 換算※] | 割合［%］ | インスタンス数 |
|---|---|---|---|---|
| J_SASEBO_ASIC_TOP | 1,404,242 | 731,376 | 100 | 289,344 |
| U_AES_RDATA1 | 2,680 | 1,396 | 0.2 | 345 |
| U_AES_RDATA2 | 2,491 | 1,297 | 0.2 | 356 |
| U_J_AES0 | 45,344 | 23,617 | 3.2 | 11,098 |
| U_J_AES1 | 36,470 | 18,995 | 2.6 | 11,940 |
| U_J_AES2 | 97,306 | 50,680 | 6.9 | 28,814 |
| U_J_AES3 | 27,110 | 14,120 | 1.9 | 6,895 |
| U_J_AES4 | 21,852 | 11,381 | 1.6 | 5,324 |
| U_J_AES5 | 46,213 | 24,069 | 3.3 | 8,732 |
| U_J_AES6 | 33,339 | 17,364 | 2.4 | 7,993 |
| U_J_AES7 | 38,663 | 20,137 | 2.8 | 5,047 |
| U_J_AES8 | 62,055 | 32,321 | 4.4 | 13,602 |
| U_J_AES9 | 131,948 | 68,723 | 9.4 | 28,769 |
| U_J_AES10 | 171,577 | 89,363 | 12.2 | 30,930 |
| U_J_AES11 | 60,260 | 31,385 | 4.3 | 12,404 |
| U_J_AES12 | 53,180 | 27,698 | 3.8 | 11,129 |
| U_J_AES13 | 33,927 | 17,671 | 2.4 | 6,083 |
| U_J_CAMELLIA | 24,927 | 12,983 | 1.8 | 7,257 |
| U_J_SEED | 35,223 | 18,345 | 2.5 | 11,179 |
| U_J_MISTY1 | 27,799 | 14,479 | 2 | 8,876 |
| U_J_T_DES | 9,612 | 5,007 | 0.7 | 2,349 |
| U_J_DES | 5,825 | 3,034 | 0.4 | 1,576 |
| U_J_CAST | 46,993 | 24,476 | 3.3 | 13,239 |
| U_J_ECC | 158,845 | 82,732 | 11.3 | 21,600 |
| U_J_RSA | 114,815 | 59,799 | 8.2 | 18,517 |
| U_J_CLEFIA | 17,364 | 9,044 | 1.2 | 4,097 |

※2 入力 NAND 換算 ＝SC43BUFXC1（1.92[um2]）単位

表 6-8　レイアウト前後の面積比較

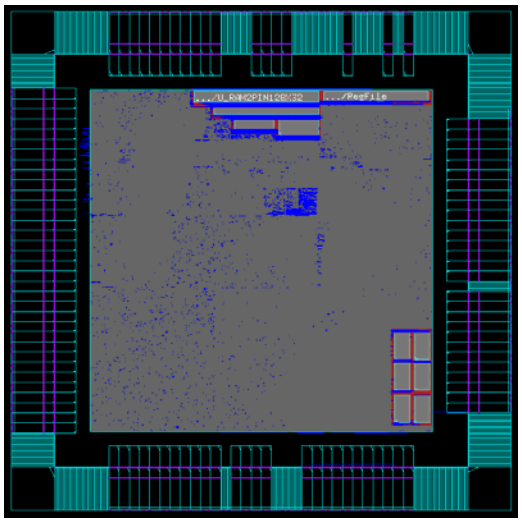
| 階層名 | レイアウト後 | | | 論理合成直後 | | |
|---|---|---|---|---|---|---|
| | セル面積 [um$^2$] | セル面積 2 入力 NAND 換算※ | 割合 [%] | セル面積 [um$^2$] | セル面積 2 入力 NAND 換算※ | 割合 [%] |
| J_SASEBO_ASIC_TOP | 1,404,242 | 731,376 | 100 | 1,387,994 | 722,914 | 100 |
| U_AES_RDATA1 | 2,680 | 1,396 | 0.2 | 1,928 | 1,004 | 0.1 |
| U_AES_RDATA2 | 2,491 | 1,297 | 0.2 | 1,928 | 1,004 | 0.1 |
| U_J_AES0 | 45,344 | 23,617 | 3.2 | 42,104 | 21,929 | 3 |
| U_J_AES1 | 36,470 | 18,995 | 2.6 | 34,969 | 18,213 | 2.5 |
| U_J_AES2 | 97,306 | 50,680 | 6.9 | 95,268 | 49,619 | 6.9 |
| U_J_AES3 | 27,110 | 14,120 | 1.9 | 25,500 | 13,281 | 1.8 |
| U_J_AES4 | 21,852 | 11,381 | 1.6 | 20,007 | 10,421 | 1.4 |
| U_J_AES5 | 46,213 | 24,069 | 3.3 | 39,274 | 20,455 | 2.8 |
| U_J_AES6 | 33,339 | 17,364 | 2.4 | 32,041 | 16,688 | 2.3 |
| U_J_AES7 | 38,663 | 20,137 | 2.8 | 37,295 | 19,424 | 2.7 |
| U_J_AES8 | 62,055 | 32,321 | 4.4 | 72,646 | 37,836 | 5.2 |
| U_J_AES9 | 131,948 | 68,723 | 9.4 | 127,345 | 66,326 | 9.2 |
| U_J_AES10 | 171,577 | 89,363 | 12.2 | 207,247 | 107,941 | 14.9 |
| U_J_AES11 | 60,260 | 31,385 | 4.3 | 56,056 | 29,196 | 4 |
| U_J_AES12 | 53,180 | 27,698 | 3.8 | 61,210 | 31,880 | 4.4 |
| U_J_AES13 | 33,927 | 17,671 | 2.4 | 38,101 | 19,845 | 2.7 |
| U_J_CAMELLIA | 24,927 | 12,983 | 1.8 | 23,230 | 12,099 | 1.7 |
| U_J_SEED | 35,223 | 18,345 | 2.5 | 33,951 | 17,683 | 2.4 |
| U_J_MISTY1 | 27,799 | 14,479 | 2 | 27,338 | 14,239 | 2 |
| U_J_T_DES | 9,612 | 5,007 | 0.7 | 8,763 | 4,564 | 0.6 |
| U_J_DES | 5,825 | 3,034 | 0.4 | 5,501 | 2,865 | 0.4 |
| U_J_CAST | 46,993 | 24,476 | 3.3 | 46,095 | 24,008 | 3.3 |
| U_J_ECC | 158,845 | 82,732 | 11.3 | 138,838 | 72,311 | 10 |
| U_J_RSA | 114,815 | 59,799 | 8.2 | 106,884 | 55,669 | 7.7 |
| U_J_CLEFIA | 17,364 | 9,044 | 1.2 | 15,576 | 8,113 | 1.1 |

※2 入力 NAND 換算 = SC43BUFXC1（1.92[um2]）単位

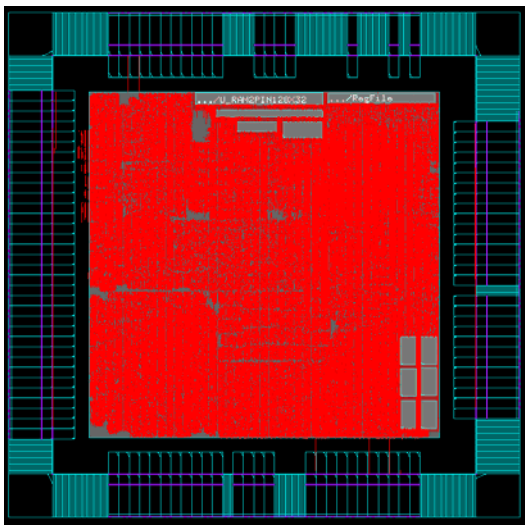
## 6.7. 信号配線

信号配線として，Metal1～Metal9 までを使用している．以下の図では，電源配線を不可視にして信号配線の様子を示している．

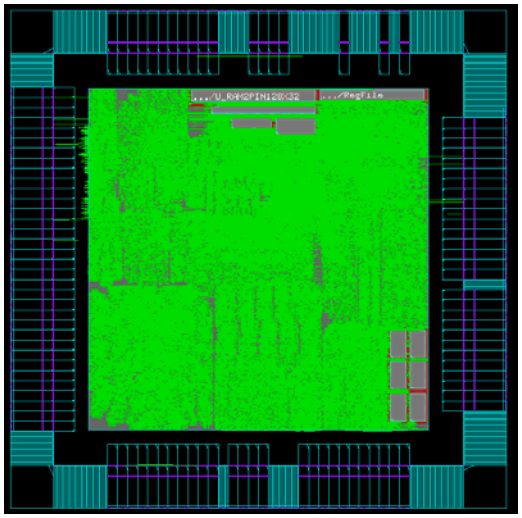
◆Metal 1



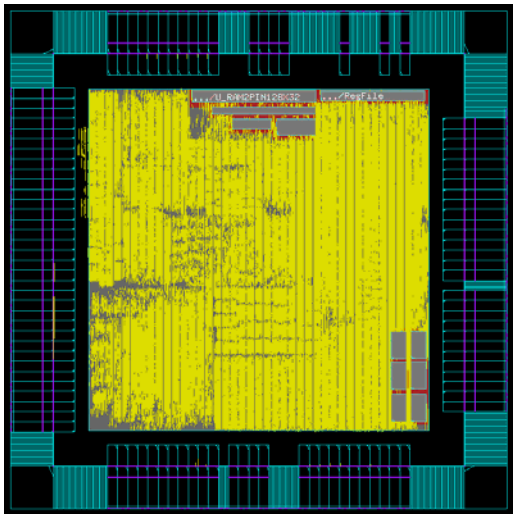
◆Metal 2



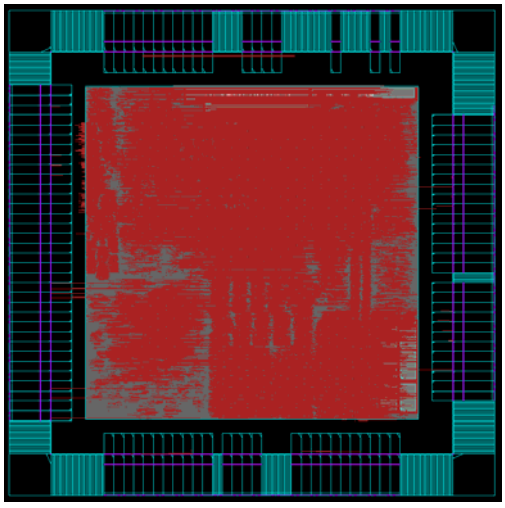
◆Metal 3



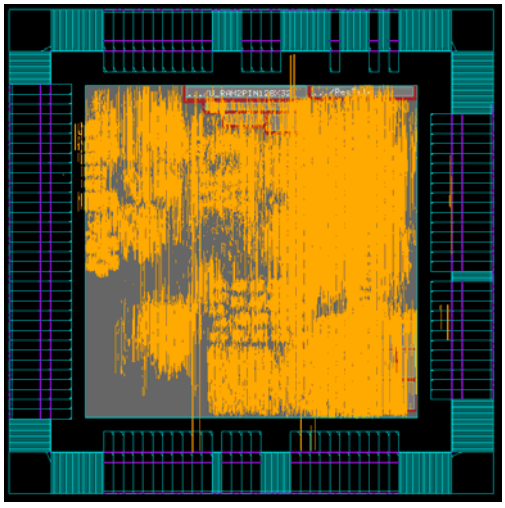
◆Metal 4



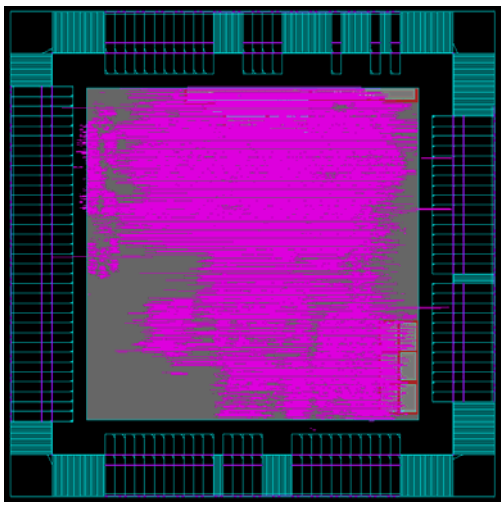
◆Metal 5



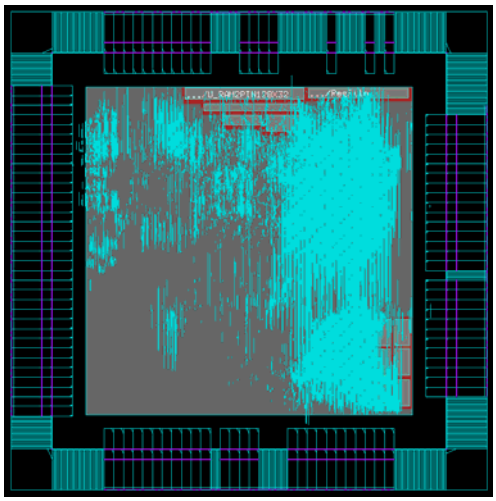
◆Metal 6



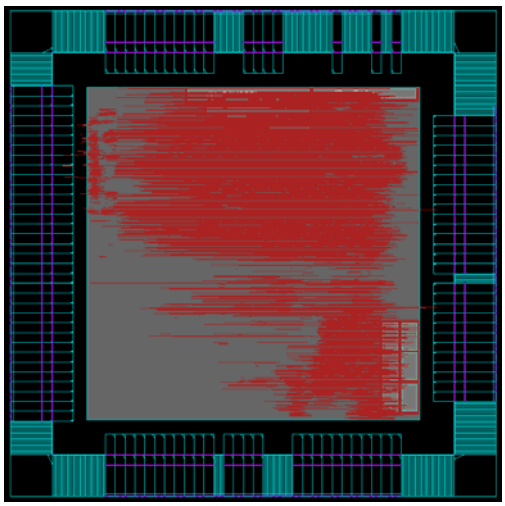
◆Metal 7



◆Metal 8



◆Metal9



## 6.8. ダミーメタル

富士通 CS202L プロセスで製造するチップのメタル層では，レイアウト中に作成する信号用・電源用配線とは別に，メタル密度制約のデザインルールを満たすためのダミーメタルパターンが配置される．図 6-8 は電源メッシュ間に配置されたダミーメタルパターンのイメージを示している．電源メッシュ間の空間内に正方形メタルパターンが敷き詰められる．正方形のサイズは以下に示すとおり，メタル層によって異なる．

Metal1 ～ Metal9 ・・・ 0.7um□
Metal10 ～ Metal11 ・・・ 1.0um□
Metal12 ・・・ 2.2um□

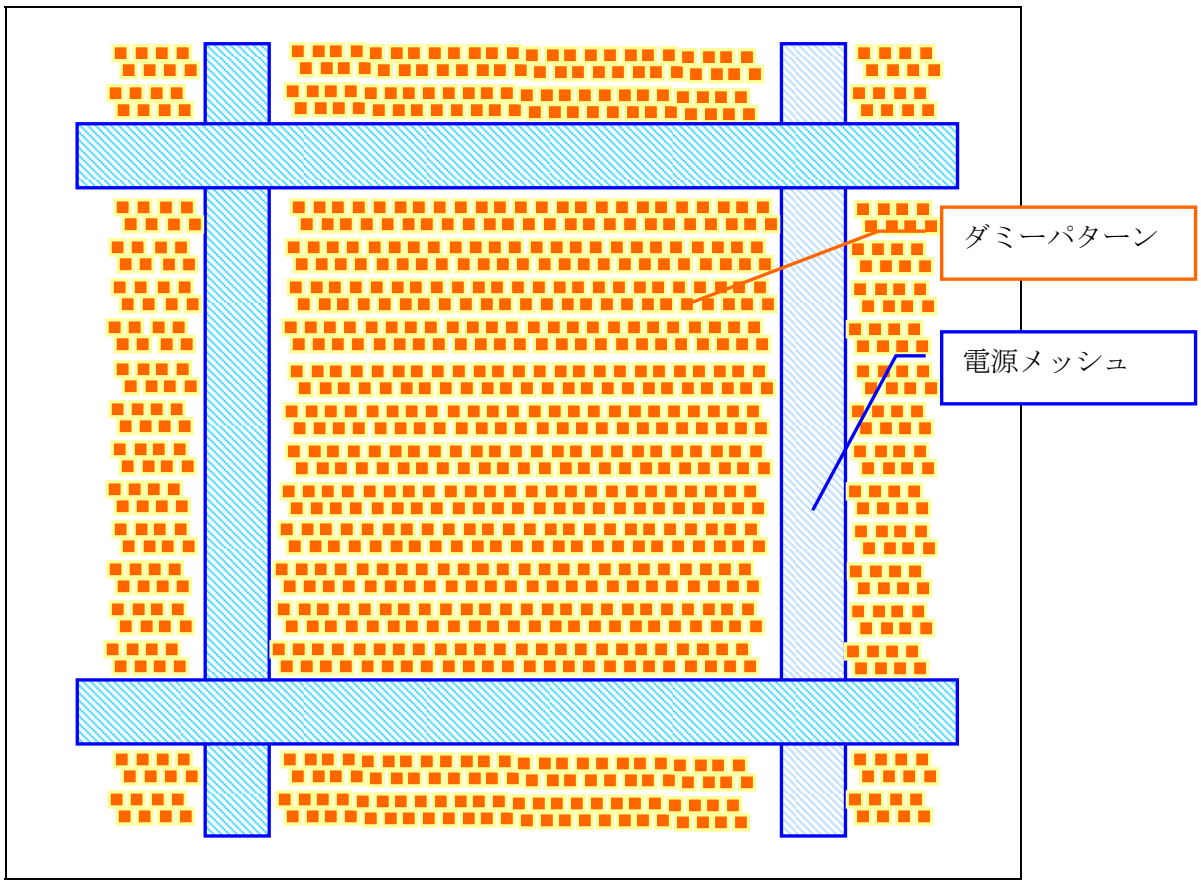



図 6-8　ダミーメタル

## 6.9. チップの方位合わせ

今回作成した暗号LSIには，チップの方位を示すため，図 6-9 のようにチップ右上角部にFマークを配置している．チップ側のパッドは，上辺右側を 1 番として反時計回りに配置されている．各パッドの信号名とセンター座標を表 6-9および表 6-10に示す．

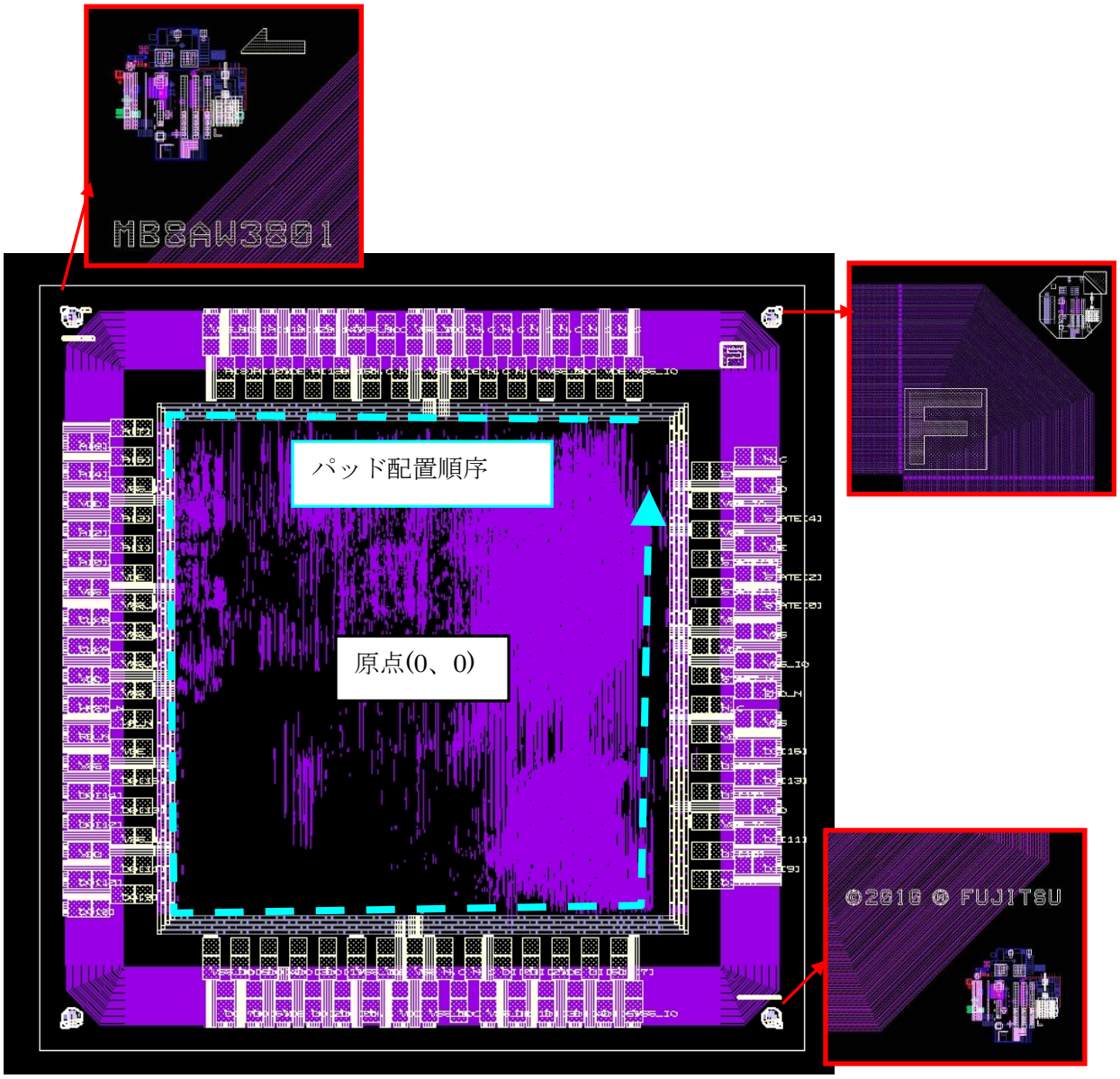



図 6-9　チップの方位合わせ

表 6-9　信号―パッドセンター座標（上辺／左辺）

| | 信号名 | ﾁｯﾌﾟﾊﾟｯﾄﾞ座標 | | | 信号名 | ﾁｯﾌﾟﾊﾟｯﾄﾞ座標 | |
|---|---|---|---|---|---|---|---|
| | | x［μm］ | y［μm］ | | | x［μm］ | y［μm］ |
| 1 | VSS_IO | 580 | 822.5 | 31 | A[7] | -822.5 | 660 |
| 2 | N.C | 540 | 939.5 | 32 | A[6] | -939.5 | 620 |
| 3 | VDE | 500 | 822.5 | 33 | A[5] | -822.5 | 580 |
| 4 | N.C | 460 | 939.5 | 34 | A[4] | -939.5 | 540 |
| 5 | N.C | 420 | 822.5 | 35 | VSS_IO | -822.5 | 500 |
| 6 | N.C | 380 | 939.5 | 36 | VDD | -939.5 | 460 |
| 7 | VSS_IO | 340 | 822.5 | 37 | A[3] | -822.5 | 420 |
| 8 | N.C | 300 | 939.5 | 38 | A[2] | -939.5 | 380 |
| 9 | N.C | 260 | 822.5 | 39 | A[1] | -822.5 | 340 |
| 10 | N.C | 220 | 939.5 | 40 | A[0] | -939.5 | 300 |
| 11 | N.C | 180 | 822.5 | 41 | VDE | -822.5 | 260 |
| 12 | N.C | 140 | 939.5 | 42 | VSS | -939.5 | 220 |
| 13 | VDE | 100 | 822.5 | 43 | VSS_IO | -822.5 | 180 |
| 14 | VDD | 60 | 939.5 | 44 | CLKB | -939.5 | 140 |
| 15 | VSS | 20 | 822.5 | 45 | VSS_IO | -822.5 | 100 |
| 16 | VSS_IO | -20 | 939.5 | 46 | CLKA | -939.5 | 60 |
| 17 | N.C | -60 | 822.5 | 47 | VSS_IO | -822.5 | 20 |
| 18 | N.C | -100 | 939.5 | 48 | VDD | -939.5 | -20 |
| 19 | N.C | -140 | 822.5 | 49 | VSS | -822.5 | -60 |
| 20 | VSS_IO | -180 | 939.5 | 50 | HRST_N | -939.5 | -100 |
| 21 | A[15] | -220 | 822.5 | 51 | WR_N | -822.5 | -140 |
| 22 | A[14] | -260 | 939.5 | 52 | RD_N | -939.5 | -180 |
| 23 | A[13] | -300 | 822.5 | 53 | VDE | -822.5 | -220 |
| 24 | A[12] | -340 | 939.5 | 54 | VSS | -939.5 | -260 |
| 25 | VDE | -380 | 822.5 | 55 | DO[15] | -822.5 | -300 |
| 26 | A[11] | -420 | 939.5 | 56 | DO[14] | -939.5 | -340 |
| 27 | A[10] | -460 | 822.5 | 57 | DO[13] | -822.5 | -380 |
| 28 | A[9] | -500 | 939.5 | 58 | DO[12] | -939.5 | -420 |
| 29 | A[8] | -540 | 822.5 | 59 | VSS_IO | -822.5 | -460 |
| 30 | VSS_IO | -580 | 939.5 | 60 | VDD | -939.5 | -500 |
| | | | | 61 | DO[11] | -822.5 | -540 |
| | | | | 62 | DO[10] | -939.5 | -580 |
| | | | | 63 | DO[9] | -822.5 | -620 |
| | | | | 64 | DO[8] | -939.5 | -660 |

VDD：コア用電源，VDE：IO 用電源，VSS：コア用 GND，VSS_IO：IO 用 GND

表 6-10　信号―パッドセンター座標（下辺／右辺）

| 番号 | 信号名 | ﾁｯﾌﾟﾊﾟｯﾄﾞ座標 | | 番号 | 信号名 | ﾁｯﾌﾟﾊﾟｯﾄﾞ座標 | |
|---|---|---|---|---|---|---|---|
| | | x［μm］ | y［μm］ | | | x［μm］ | y［μm］ |
| 65 | VSS_IO | -580 | -822.5 | 95 | DI[8] | 822.5 | -580 |
| 66 | DO[7] | -540 | -939.5 | 96 | DI[9] | 939.5 | -540 |
| 67 | DO[6] | -500 | -822.5 | 97 | DI[10] | 822.5 | -500 |
| 68 | DO[5] | -460 | -939.5 | 98 | DI[11] | 939.5 | -460 |
| 69 | DO[4] | -420 | -822.5 | 99 | VSS_IO | 822.5 | -420 |
| 70 | VDE | -380 | -939.5 | 100 | VDD | 939.5 | -380 |
| 71 | DO[3] | -340 | -822.5 | 101 | DI[12] | 822.5 | -340 |
| 72 | DO[2] | -300 | -939.5 | 102 | DI[13] | 939.5 | -300 |
| 73 | DO[1] | -260 | -822.5 | 103 | DI[14] | 822.5 | -260 |
| 74 | DO[0] | -220 | -939.5 | 104 | DI[15] | 939.5 | -220 |
| 75 | VSS_IO | -180 | -822.5 | 105 | VDE | 822.5 | -180 |
| 76 | N.C | -140 | -939.5 | 106 | VSS | 939.5 | -140 |
| 77 | VDE | -100 | -822.5 | 107 | N.C | 822.5 | -100 |
| 78 | VDD | -60 | -939.5 | 108 | END_N | 939.5 | -60 |
| 79 | VSS | -20 | -822.5 | 109 | START_N | 822.5 | -20 |
| 80 | VSS_IO | 20 | -939.5 | 110 | VSS_IO | 939.5 | 20 |
| 81 | N.C | 60 | -822.5 | 111 | VDD | 822.5 | 60 |
| 82 | N.C | 100 | -939.5 | 112 | VSS | 939.5 | 100 |
| 83 | N.C | 140 | -822.5 | 113 | VSS_IO | 822.5 | 140 |
| 84 | VSS_IO | 180 | -939.5 | 114 | STATE[0] | 939.5 | 180 |
| 85 | DI[0] | 220 | -822.5 | 115 | STATE[1] | 822.5 | 220 |
| 86 | DI[1] | 260 | -939.5 | 116 | STATE[2] | 939.5 | 260 |
| 87 | DI[2] | 300 | -822.5 | 117 | STATE[3] | 822.5 | 300 |
| 88 | DI[3] | 340 | -939.5 | 118 | VDE | 939.5 | 340 |
| 89 | VDE | 380 | -822.5 | 119 | VSS | 822.5 | 380 |
| 90 | DI[4] | 420 | -939.5 | 120 | STATE[4] | 939.5 | 420 |
| 91 | DI[5] | 460 | -822.5 | 121 | VSS_IO | 822.5 | 460 |
| 92 | DI[6] | 500 | -939.5 | 122 | VDD | 939.5 | 500 |
| 93 | DI[7] | 540 | -822.5 | 123 | EXEC | 822.5 | 540 |
| 94 | VSS_IO | 580 | -939.5 | 124 | N.C | 939.5 | 580 |

VDD：コア用電源，VDE：IO 用電源，VSS：コア用 GND，VSS_IO：IO 用 GND

## 6.10. 電源分離確認結果

電源 PAD からメタル配線上を走査し，他の電源や信号配線とショートが起きていないことを確認した．図 6-10 は電源層の配線パターンを抽出したものである．

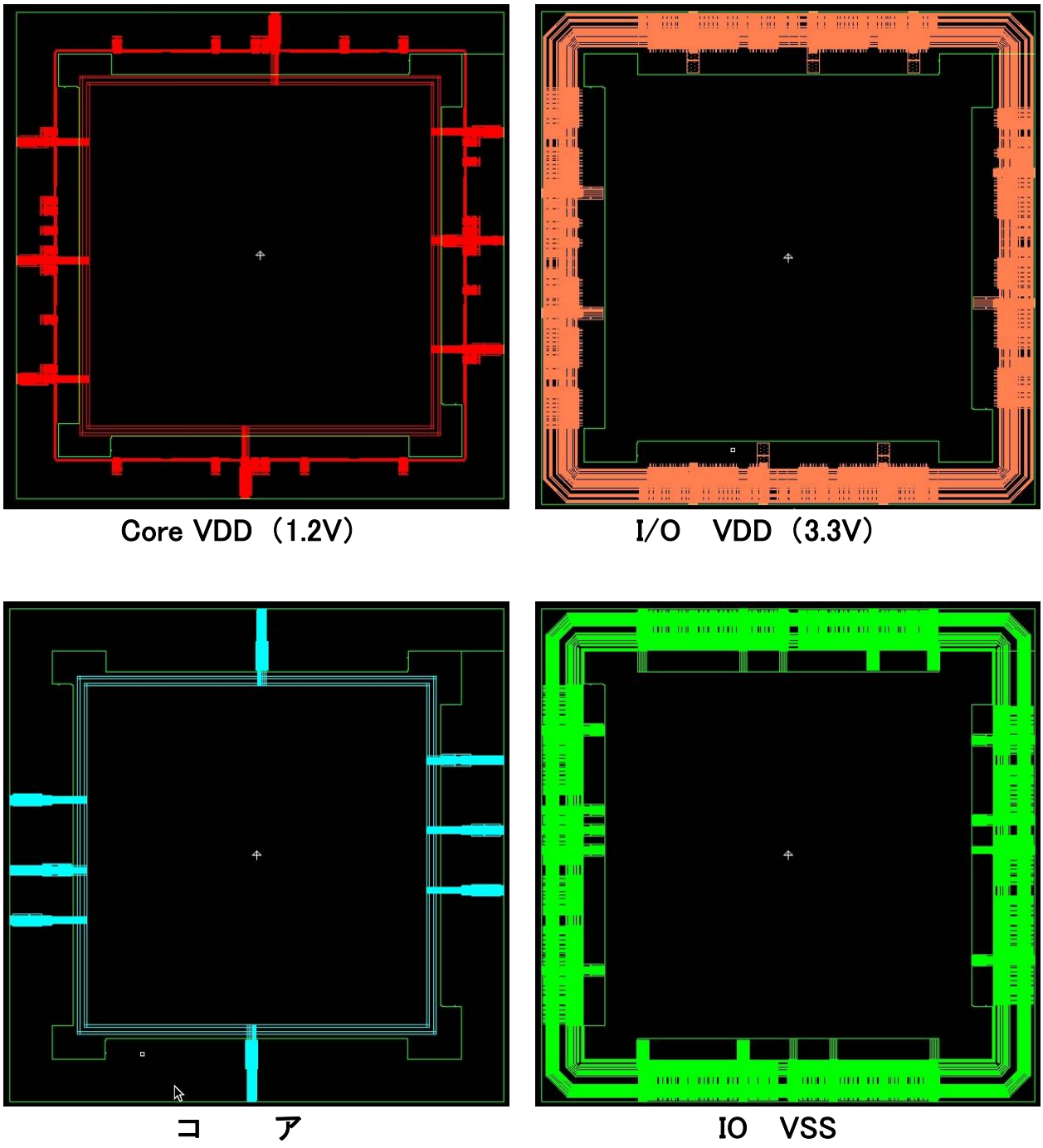



図 6-10　電源分離テスト

# 7. IR-Drop検証

図 7-1は，全セルのうちの 30%が活性化したと仮定した場合の，VDD側とVSS側のコア電源プレーンの電源降下のイメージを示している．ドロップ検証の結果を表 7-1に示す．電圧降下率はVDDで 0.3985%, VSSで 0.4455% と極めて小さいうえ，実際には同時に動作する暗号モジュールは 1 個であるため，通常動作において問題とならない値である．静的タイミング解析（STA）時には，これらの値以上の動作マージンを与えて検証を行っている．

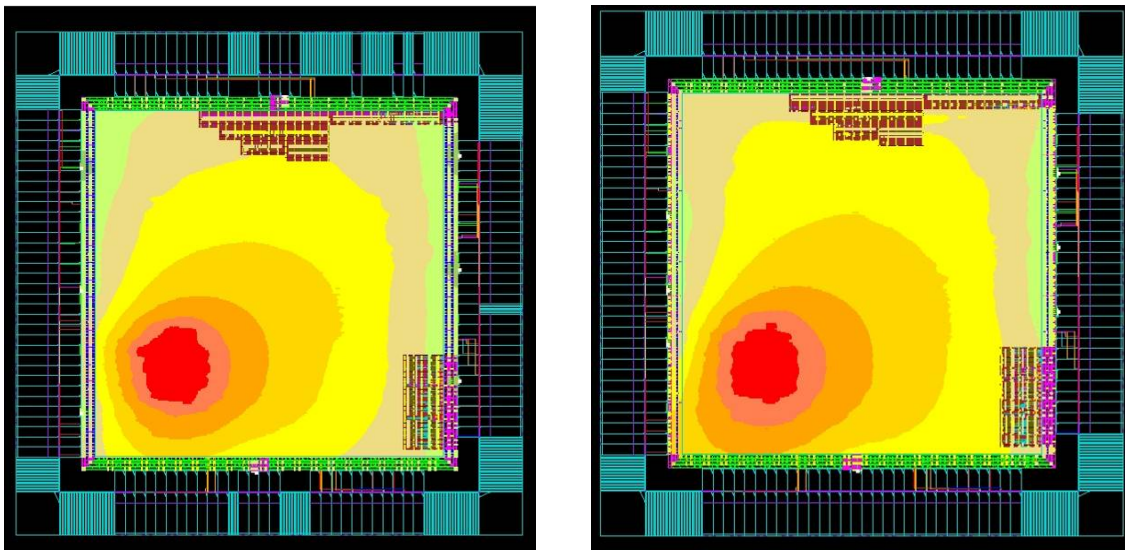


図 7-1　VDD の Drop（左）と VSS の Drop（右）

表 7-1　VDD および VSS のドロップ検証

| | VDD | VSS |
|---|---|---|
| 動作周波数 | 24MHz | |
| 動作条件 | best (1.3V, -40℃) | |
| Primary Input Activity | 30% | |
| Sequential Element Activity | 10% | |
| Clock Gates Enable Activity | 10% | |
| 消費電力 | 106 mW | 106 mW |
| Worst Drop 値 | 5.18 mV | 5.791 mV |
| Drop 率 | 0.3985% | 0.4455% |

# 8. クロストークノイズ検証

## 8.1. クロストークノイズ検証について

距離が長く並行する信号配線において，動作状態のネット（アグレッサ・ネット）が隣接する静止状態のネット（ビクティム・ネット）に影響を与え，静止状態のネットが誤作動（Noise エラー）を起こすことがある．クロストークノイズ検証では，こうした並行配線間でのノイズにより誤作動する恐れがあるかを検証する．

製造ばらつき 4 種類（tc, tcw, capb, capw）と，7 つの動作条件（worst, worstLT, nominal, nomirworst, nomirworstLT, best, bestHT）を考慮し，計 28 通りの検証を行った．閾値はライブラリ値を使用している．

## 8.2. 検証結果

クロストークノイズ検証の結果，28 通りの全条件において Noise エラーが発生しないことを確認した．一例として，下記に製造条件 capb の結果を記載する．

◆ worst 条件（1.05V、125℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                      = coupling analysis with RCs
#   Process                       = 65nm
# Failure Thresholds
#   Functional (sequential)       = 0.26 V
#   Functional (combinatorial)    = 0.84 V
#   Delay absolute                = 1000.00 ps
#   Delay relative                = 0.50
#   Slope                         = 0.00
# Number of glitch ECO failures   = 0
# Number of delay  ECO failures   = 0
# Number of slope  ECO failures   = 0
# Number of ECOs skipped          = 0
# For complete details, view the html or text ECO report
# ********************************************************************
```

◆ worstLT 条件（1.05V、－40℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                      = coupling analysis with RCs
#   Process                       = 65nm
# Failure Thresholds
#   Functional (sequential)       = 0.26 V
#   Functional (combinatorial)    = 0.84 V
#   Delay absolute                = 1000.00 ps
#   Delay relative                = 0.50
#   Slope                         = 0.00
# Number of glitch ECO failures   = 0
# Number of delay  ECO failures   = 0
# Number of slope  ECO failures   = 0
```

```
# Number of ECOs skipped           = 0
# For complete details, view the html or text ECO report
#*********************************************************************
```

◆ nonirworst 条件（1.1V、125℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                       = coupling analysis with RCs
#   Process                        = 65nm
# Failure Thresholds
#   Functional (sequential)        = 0.28 V
#   Functional (combinatorial)     = 0.88 V
#   Delay absolute                 = 1000.00 ps
#   Delay relative                 = 0.50
#   Slope                          = 0.00
# Number of glitch ECO failures    = 0
# Number of delay  ECO failures    = 0
# Number of slope  ECO failures    = 0
# Number of ECOs skipped           = 0
# For complete details, view the html or text ECO report
# *********************************************************************
```

◆ nonirworstLT 条件（1.1V、－40℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                       = coupling analysis with RCs
#   Process                        = 65nm
# Failure Thresholds
#   Functional (sequential)        = 0.28 V
#   Functional (combinatorial)     = 0.88 V
#   Delay absolute                 = 1000.00 ps
#   Delay relative                 = 0.50
#   Slope                          = 0.00
# Number of glitch ECO failures    = 0
# Number of delay  ECO failures    = 0
# Number of slope  ECO failures    = 0
# Number of ECOs skipped           = 0
# For complete details, view the html or text ECO report
# *********************************************************************
```

◆ nominal 条件（1.2V、25℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                       = coupling analysis with RCs
#   Process                        = 65nm
# Failure Thresholds
```

```
#   Functional (sequential)         = 0.30 V
#   Functional (combinatorial)      = 0.96 V
#   Delay absolute                  = 1000.00 ps
#   Delay relative                  = 0.50
#   Slope                           = 0.00
# Number of glitch ECO failures     = 0
# Number of delay  ECO failures     = 0
# Number of slope  ECO failures     = 0
# Number of ECOs skipped            = 0
# For complete details, view the html or text ECO report
# ********************************************************************
```

◆ best 条件（1.3V、－40℃）での Noise 検証結果

```
**********************************************************************
# Run settings
#   Run mode                        = coupling analysis with RCs
#   Process                         = 65nm
# Failure Thresholds
#   Functional (sequential)         = 0.33 V
#   Functional (combinatorial)      = 1.04 V
#   Delay absolute                  = 1000.00 ps
#   Delay relative                  = 0.50
#   Slope                           = 0.00
# Number of glitch ECO failures     = 0
# Number of delay  ECO failures     = 0
# Number of slope  ECO failures     = 0
# Number of ECOs skipped            = 0
# For complete details, view the html or text ECO report
**********************************************************************
```

◆ bestHT 条件（1.3V、125℃）での Noise 検証結果

```
**********************************************************************
# # Run settings
#   Run mode                        = coupling analysis with RCs
#   Process                         = 65nm
# Failure Thresholds
#   Functional (sequential)         = 0.33 V
#   Functional (combinatorial)      = 1.04 V
#   Delay absolute                  = 1000.00 ps
#   Delay relative                  = 0.50
#   Slope                           = 0.00
# Number of glitch ECO failures     = 0
# Number of delay  ECO failures     = 0
# Number of slope  ECO failures     = 0
# Number of ECOs skipped            = 0
# For complete details, view the html or text ECO report
#
**********************************************************************
```

# 9. STA検証

## 9.1. 検証条件と結果

表 9-1および表 9-2に示す条件で静的タイミング解析を実施した. その結果, すべてのSetupおよびHoldでタイミングエラーは生じなかった. ただし, Clock Gatingの箇所表示されるエラーは疑似的なものとして扱う. これについての詳細は9.2節を参照のこと. クロックのスペックについては, 9.3節を参照のこと.

表 9-1　STA 条件

| | | |
|---|---|---|
| 使用ツール | | PrimetimeSI |
| 使用ネット | | J_SASEBO_ASIC_TOP.v |
| プロセス条件 | | tc, tcw, capw, capb |
| 動作条件 | | best (1.3V / -40℃) |
| | | bestHT (1.3V / 125℃) |
| | | worst (1.05V / 125℃) |
| | | worstLT (1.05V / -40℃) |
| | | nonirworst (1.1V / 125℃) |
| | | nonirworstLT (1.1V / -40℃) |
| | | nominal (1.2V / 25℃) |
| STA 制約 | 設定周波数 | 24MHz (41666 ps) |
| | 入力遅延値 | 2000 ps |
| | 出力遅延値 | 2000 ps |
| | Derate Factor | 表 9-2参照 |
| | False Path | CLKAドメイン ⇔ CLKBドメイン |

表 9-2　Derate Factor

| COND | -net_delay | | -cell_delay | | set_clock_uncertainty[ps] |
|---|---|---|---|---|---|
| | early | late | early | late | |
| best / bestHT | 0.93 | 1 | 0.95 | 1.07 | 10 |
| worst / worstLT<br>nonirworst / nonirworstLT | 0.93 | 1 | 0.9 | 1.04 | 10 |
| nominal | 1 | 1 | 1 | 1 | 10 |

## 9.2. Clock Gating Timing Error概要

### 9.2.1 発生箇所

表 9-3に示すCTS ROOT Cell において Clock Gating のHold Violation が発生した.

表 9-3　Clock Gating の Hold Violation の発生箇所

| | | |
|---|---|---|
| U_AES0_CLK_GATE | U_AES9_CLK_GATE | U_MISTY1_CLK_GATE |
| U_AES1_CLK_GATE | U_AES10_CLK_GATE | U_T_DES_CLK_GATE |
| U_AES2_CLK_GATE | U_AES11_CLK_GATE | U_DES_CLK_GATE |
| U_AES3_CLK_GATE | U_AES12_CLK_GATE | U_CAST_CLK_GATE |
| U_AES4_CLK_GATE | U_AES13_CLK_GATE | U_ECC_CLK_GATE |
| U_AES5_CLK_GATE | U_AES_RDATA1_CLK_GATE | U_RSA_CLK_GATE |
| U_AES6_CLK_GATE | U_AES_RDATA2_CLK_GATE | U_CLEFIA_CLK_GATE |
| U_AES7_CLK_GATE | U_CAMELLIA_CLK_GATE | |
| U_AES8_CLK_GATE | U_SEED_CLK_GATE | |

### 9.2.2 Clock Gating Timing Error の問題点

Clock Gating で Hold Violation が発生すると，ハザードや狭いクロックが生成され回路動作に影響を与える恐れがある（図 9-1 参照）．

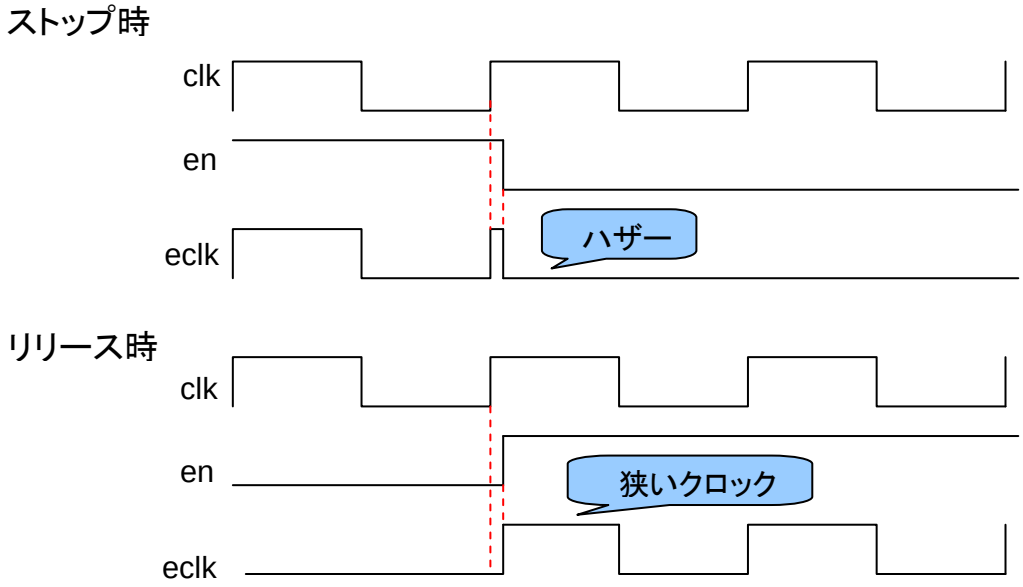



図 9-1　ハザードおよび狭いクロックの発生

今回作成した暗号 LSI では，en 信号が変化するのは数 μ sec 続くリセット状態のときのみで，ハザードや狭いクロックが出た後にリセット状態に入るため回路への影響はない（図 9-2 参照）．

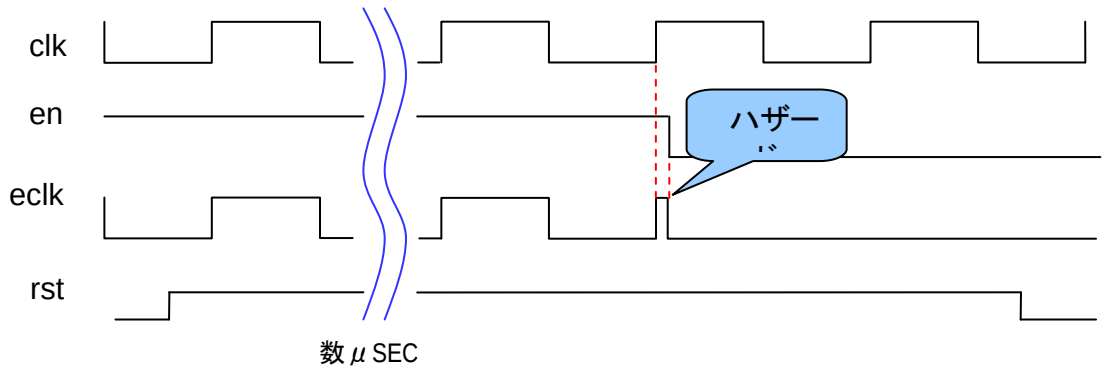



図 9-2　リセット状態におけるハザードの発生

## 9.3. 最大動作速度

STA での最大動作速度を以下に示す．赤字は全条件中のワースト値を表している．最終データを用いてクロストークを考慮した静的タイミング解析を行い，すべての条件で Setup/Hold タイミングエラーが発生しないことを確認した．

表 9-4　PROCESS = capb

| COND | CLKA | | | CLKB | | |
|---|---|---|---|---|---|---|
| | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] |
| worst | 13,771.5 | 35.8 | 36.5 | 39,011.0 | 376.6 | 131.6 |
| worstLT | 14,547.1 | 36.9 | 4.3 | 39,354.9 | 432.7 | 102.4 |
| nonirworst | 14,353.0 | 36.6 | 36.8 | 39,223.4 | 409.4 | 125.2 |
| nonirworstLT | 15,182.3 | 37.8 | **1.7** | 39,580.8 | 479.6 | 101.4 |
| nominal | 16,693.6 | 40.0 | 20.0 | 40,081.3 | 631.0 | 112.5 |
| best | 17,951.2 | 42.2 | 27.1 | 40,495.1 | 854.0 | 86.0 |
| bestHT | 17,407.8 | 41.2 | 37.9 | 40,224.4 | 693.7 | **81.4** |

表 9-5　PROCESS = capw

| COND | CLKA | | | CLKB | | |
|---|---|---|---|---|---|---|
| | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] |
| worst | **13,201.4** | **35.1** | 46.7 | **38,674.4** | **334.3** | 153.1 |
| worstLT | 14,044.0 | 36.2 | 13.2 | 39,072.7 | 385.6 | 146.6 |
| nonirworst | 13,833.4 | 35.9 | 47.9 | 38,918.2 | 363.9 | 156.1 |
| nonirworstLT | 14,737.0 | 37.1 | 8.6 | 39,327.5 | 427.6 | 141.6 |
| nominal | 16,382.8 | 39.6 | 17.4 | 39,881.6 | 560.4 | 143.5 |
| best | 17,730.6 | 41.8 | 27.5 | 40,351.7 | 760.9 | 93.4 |
| bestHT | 17,145.6 | 40.8 | 42.7 | 40,031.5 | 611.8 | 106.3 |

表 9-6　PROCESS = tc

| COND | CLKA | | | CLKB | | |
|---|---|---|---|---|---|---|
| | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] |
| worst | 13,507.1 | 35.5 | 42.3 | 38,857.3 | 356.0 | 152.3 |
| worstLT | 14,313.5 | 36.6 | 8.4 | 39,222.7 | 409.3 | 124.1 |
| nonirworst | 14,112.6 | 36.3 | 42.2 | 39,082.3 | 387.0 | 154.0 |
| nonirworstLT | 14,977.8 | 37.5 | 4.7 | 39,466.5 | 454.7 | 118.9 |
| nominal | 16,551.2 | 39.8 | 26.1 | 39,987.0 | 595.6 | 126.6 |
| best | 17,850.5 | 42.0 | 29.7 | 40,430.0 | 809.1 | 89.6 |
| bestHT | 17,288.8 | 41.0 | 40.7 | 40,137.1 | 654.1 | 93.5 |

表 9-7　PROCESS = tcw

| COND | CLKA | | | CLKB | | |
|---|---|---|---|---|---|---|
| | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] | SETUP[ps] | 最大動作周波数[MHz] | HOLD[ps] |
| worst | 13,698.6 | 35.8 | 38.3 | 38,944.2 | 367.4 | 144.5 |
| worstLT | 14,477.3 | 36.8 | 5.6 | 39,294.4 | 421.7 | 110.8 |
| nonirworst | 14,286.7 | 36.5 | 38.5 | 39,160.3 | 399.1 | 136.8 |
| nonirworstLT | 15,109.3 | 37.7 | 15.0 | 39,530.2 | 468.2 | 108.0 |
| nominal | 16,638.9 | 40.0 | 21.3 | 40,043.0 | 616.2 | 116.8 |
| best | 17,912.5 | 42.1 | 26.9 | 40,464.9 | 832.5 | 85.8 |
| bestHT | 17,363.8 | 41.1 | 38.4 | 40,186.9 | 676.1 | 82.8 |

### 9.4. Not Annotated解析

配線に対して実負荷容量情報が考慮されていない Net が存在する場合，Not Annotated がレポートされる．通常配線が Not Annotated になってしまうと，寄生容量情報が STA で考慮されず，正しいタイミング検証が行われない．ただし，VDD，VSS へ接続しているネット（TIE Hi/ TIE Lo）や，実際には使用されていないポート(UNCONNECT/ FLOAT_PIN)などは，STA 上で Timing Arc を持たないため問題ない．

検証の結果，通常配線に Not Annotated は存在していないことから，正しい実負荷容量のもとで STA が行われたと言える．以下に解析結果を示す．

## 10. 形式検証

作成したRTLとレイアウト後最終ネットリストで形式検証を行い，機能的に等価であることを確認した．検証結果の抜粋を図 10-1に示す．等価検証実行ログにSUCCEEDEDの記述があり，RTLとネットリストは機能的に等価であることが確認された．

```
********************************** Verification Results **********************************
Verification SUCCEEDED
   ATTENTION:  synopsys_auto_setup mode was enabled.
               See Synopsys Auto Setup Summary for details.
   ATTENTION: RTL interpretation messages were produced during link
              of reference design.
              Verification results may disagree with a logic simulator.
------------------------------------------------------------------------

 Reference design: r:/WORK/J_SASEBO_ASIC_TOP
 Implementation design: i:/WORK/J_SASEBO_ASIC_TOP
 25079 Passing compare points
------------------------------------------------------------------------------------------

Matched Compare Points     BBPin    Loop   BBNet     Cut     Port     DFF      LAT    TOTAL
------------------------------------------------------------------------------------------

Passing (equivalent)        1109       0       0       0       24   23946        0    25079
Failing (not equivalent)       0       0       0       0        0       0        0        0
******************************************************************************************
```

図 10-1　形式検証の実行ログの抜粋

```
                    |         |         |          |    RC    |   Not    |
Net Type            |  Total  | Lumped  |  RC pi   | network  |Annotated|
--------------------+---------+---------+----------+----------+----------+
Internal nets       |         |         |          |          |          |
  - Pin to pin nets |  290937 |       0 |        0 |  290918  |       19 |
  - Driverless nets |    5297 |       0 |        0 |        0 |     5297 |
  - Loadless nets   |     111 |       6 |        0 |        0 |      105 |
--------------------+---------+---------+----------+----------+----------+
Boundary/port nets  |         |         |          |          |          |
  - Pin to pin nets |      61 |       0 |        0 |       61 |        0 |
  - Driverless nets |       0 |       0 |        0 |        0 |        0 |
  - Loadless nets   |       0 |       0 |        0 |        0 |        0 |
--------------------+---------+---------+----------+----------+----------+
                    |  296406 |       6 |        0 |  290979  |    5421  |
```

Not Annotated ネットの内訳
Pin to pin nets + Loadless nets = 124 = TIEHi ネット(28) + TIELo ネット(96)
Driverless nets = 5297 = UNCONNECT(2116) + FLOAT_PIN(3171)

# 11. レイアウト検証

## 11.1. DRC

Calibre v2008.3_16.12 を使用し，回路のデザインルールチェック(DRC)を行った．検証環境を表 11-1に示す．DRCの結果，富士通CS202 プロセスにおけるデザインルールをすべて満たしていることが確認された．DRCの実行結果を図 11-1に抜粋する．

表 11-1　DRC 実行環境

| | |
|---|---|
| 使用ツール (Version) | Calibre (v2008.3_16.12) |
| GDS ファイル名 | MB8AW3801_10031701.gds |
| トップセル名 | MB8AW3801 |
| ルールファイル名 | MB8AW3801_drc.rul |
| ルールバージョン | r2.91 |

```
================================================================================ CALIBRE::DRC-H
SUMMARY REPORT
===
Execution Date/Time:        Wed Mar 17 13:46:42 2010
Calibre Version:            v2008.3_16.12    Tue Aug 19 13:58:10 PDT 2008
Rule File Pathname:         MB8AW3801_drc.rul
Rule File Title:
Layout System:              GDS
Layout Path(s):             MB8AW3801_10031701.gds
Layout Primary Cell:        MB8AW3801
Excluded Cells:

--- RULECHECK RESULTS STATISTICS

--- RULECHECK RESULTS STATISTICS (BY CELL)

--- SUMMARY
---
TOTAL CPU Time:                  10434
TOTAL REAL Time:                 10523
TOTAL Original Layer Geometries: 3772023 (111217971)
TOTAL DRC RuleChecks Executed:   2756
TOTAL DRC Results Generated:     0 (0)
```

図 11-1　DRC 実行結果の抜粋

## 11.2. ANT

製造工程時のアンテナ効果によるゲート破壊を起こす配線が存在するか，確認を行った．検証実行環境を表 11-2に示す．その結果，ゲート破壊を起こす配線は確認されなかった．図 11-2に検証結果の一部を抜粋する．

表 11-2　ANT 検証環境

| | |
|---|---|
| 使用ツール (Version) | Calibre (v2008.3_16.12) |
| GDS ファイル名 | MB8AW3801_10031701.gds |
| トップセル名 | MB8AW3801 |
| ルールファイル名 | MB8AW3801_ant.rul |
| ルールバージョン | r2.91 |

```
================================================================================ CALIBRE::DRC-H
SUMMARY REPORT
===
Execution Date/Time:        Wed Mar 17 13:46:42 2010
Calibre Version:            v2008.3_16.12     Tue Aug 19 13:58:10 PDT 2008
Rule File Pathname:         MB8AW3801_drc.rul
Rule File Title:
Layout System:              GDS
Layout Path(s):             MB8AW3801_10031701.gds
Layout Primary Cell:        MB8AW3801
Excluded Cells:

--- RULECHECK RESULTS STATISTICS

--- RULECHECK RESULTS STATISTICS (BY CELL)

--- SUMMARY
---
TOTAL CPU Time:                  10434
TOTAL REAL Time:                 10523
TOTAL Original Layer Geometries: 3772023 (111217971)
TOTAL DRC RuleChecks Executed:   2756
TOTAL DRC Results Generated:     0 (0)
```

図 11-2　ANT 検証結果の抜粋

## 11.3. DFM

DFM (Design for Manufacturability) 検証は，チップ製造の歩留まり向上を目的としたレイアウト検証である．検証実行環境を表 11-3に示す．．富士通支給のデフォルト設定では，エラーは確認されなかった． 図 11-3図 11-3に検証結果の一部を抜粋する．

表 11-3　DFM 検証環境

| | |
|---|---|
| 使用ツール (Version) | Calibre (v2008.3_16.12) |
| GDS ファイル名 | MB8AW3801_10031701.gds |
| トップセル名 | MB8AW3801 |
| ルールファイル名 | MB8AW3801_dfm.rul |
| ルールバージョン | r2.91 |

```
================================================================================   CALIBRE::DRC-H
SUMMARY REPORT
===
Execution Date/Time:        Wed Mar 17 13:46:42 2010
Calibre Version:            v2008.3_16.12     Tue Aug 19 13:58:10 PDT 2008
Rule File Pathname:         MB8AW3801_drc.rul
Rule File Title:
Layout System:              GDS
Layout Path(s):             MB8AW3801_10031701.gds
Layout Primary Cell:        MB8AW3801
Excluded Cells:

--- RULECHECK RESULTS STATISTICS

--- RULECHECK RESULTS STATISTICS (BY CELL)

--- SUMMARY
---
TOTAL CPU Time:                  10434
TOTAL REAL Time:                 10523
TOTAL Original Layer Geometries: 3772023 (111217971)
TOTAL DRC RuleChecks Executed:   2756
TOTAL DRC Results Generated:     0 (0)
```

図 11-3　DFM 検証結果の抜粋

## 11.4. FL

FL検証は，富士通 65nm CS202Lプロセスにおける暫定DRC項目である．FL検証は，FLレイヤー（拡散層）の密度について，特殊なケースが起こり得るかを確認する．検証実行環境を表 11-4に示す．検証の結果，本レイアウトではこのようなケースが生じなかった．図 11-4に検証結果の一部を抜粋する．

表 11-4　FL 検証環境

| | |
|---|---|
| 使用ツール (Version) | Calibre (v2008.3_16.12) |
| GDS ファイル名 | MB8AW3801_10031701.gds |
| トップセル名 | MB8AW3801 |
| ルールファイル名 | J_SASEBO_ASIC_TOP.rul |
| ルールバージョン | r2.91 |

```
================================================================================
=== CALIBRE::DRC-H SUMMARY REPORT
===
Execution Date/Time:        Wed Mar 17 17:22:06 2010
Calibre Version:            v2008.3_16.12     Tue Aug 19 13:58:10 PDT 2008
Rule File Pathname:         J_SASEBO_ASIC_TOP.rul
Rule File Title:
Layout System:              GDS
Layout Path(s):             MB8AW3801_10031701.gds
Layout Primary Cell:        MB8AW3801
Excluded Cells:

--- RULECHECK RESULTS STATISTICS
--- RULECHECK RESULTS STATISTICS (BY CELL)
--- SUMMARY
---
TOTAL CPU Time:                   94
TOTAL REAL Time:                  340
TOTAL Original Layer Geometries: 21084 (20374350)
TOTAL DRC RuleChecks Executed:    1
TOTAL DRC Results Generated:      0 (0)
```

図 11-4　FL 検証結果の抜粋

## 11.5. LVS

LVS (Layout Versus Schematic) 検証は，レイアウトデータ(.GDS)からトランジスタレベルの接続情報を抽出し，ネットリスト(.v)の接続情報と一致しているかを検証する．検証実行環境を表 11-5 に示す．検証の結果，レイアウトデータとネットリストが等価であることが確認された．LVS検証の実行結果を図 11-5に抜粋する．

表 11-5　LVS 検証環境

| | |
|---|---|
| 使用ツール (Version) | Calibre (v2008.3_16.12) |
| GDS ファイル名 | MB8AW3801_10031701.gds |
| 検証対象ネット名 | J_SASEBO_ASIC_TOP_lsv.v |
| Source CDL 名 | J_SASEBO_ASIC_TOP.cdl |
| レイアウト側トップセル名 | MB8AW3801 |
| ソース側トップセル名 | J_SASEBO_ASIC_TOP |
| ルールファイル名 | MB8AW3801_lvs.rul |
| ルールバージョン | r2.91 |

```
REPORT FILE NAME:       MB8AW3801_lvs.sum
LAYOUT NAME:            MB8AW3801.layout_net.gz ('MB8AW3801')
SOURCE NAME:            J_SASEBO_ASIC_TOP.cdl ('J_SASEBO_ASIC_TOP')
RULE FILE:              MB8AW3801_lvs.rul
CREATION TIME:          Wed Mar 17 17:31:33 2010
CURRENT DIRECTORY:      backend/AIST/j_sasebo3_FUJITSU_65nm/Calibre/LVS
CALIBRE VERSION:        v2008.3_16.12     Tue Aug 19 13:58:10 PDT 2008

                    OVERALL COMPARISON RESULTS

        #       ##################        _   _
       #        #                #       *   *
    #   #       #     CORRECT    #         |
     # #        #                #       ¥___/
      #         ##################
```

図 11-5　LVS 検証結果の抜粋

## 12. 検証結果のまとめ

各検証結果について以下にまとめる.

| | | |
|---|---|---|
| STA 検証: | setup/hold | エラーなし |
| X-Talk (Noise) 検証: | Noise エラー | エラーなし |
| Power 検証: | IR-Drop | 0.8535% ⇒ 動作マージンを考慮して STA 実行 |
| | VDD | 0.3985% |
| | VSS | 0.4456% |
| | 電源分離 | 各電源でのショートなし |
| レイアウト検証: | DRC | エラーなし |
| | ANT | エラーなし |
| | DFM | エラーなし |
| | FL | エラーなし |
| | LVS | Netlist とレイアウトの一致を確認 |
| Netlist 等価検証: | 等価検証 | 最終 RTL と最終ネットの等価を確認 |

以上より, すべての検証で問題ないことが確認された.

# 13. 暗号ハードウェアIPコア

## 13.1. AES0 (合成体S-box)

AES暗号マクロAES0の概要を表13-1に，I/Oポートを表13-2に示す．AESは米国NISTによって標準化された共通鍵ブロック暗号であり，ISO/IEC18033でも標準化されている[1)]．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 13-1　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 13-2　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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

AES0 は図 13-1に示した暗号化回路と図 13-2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.

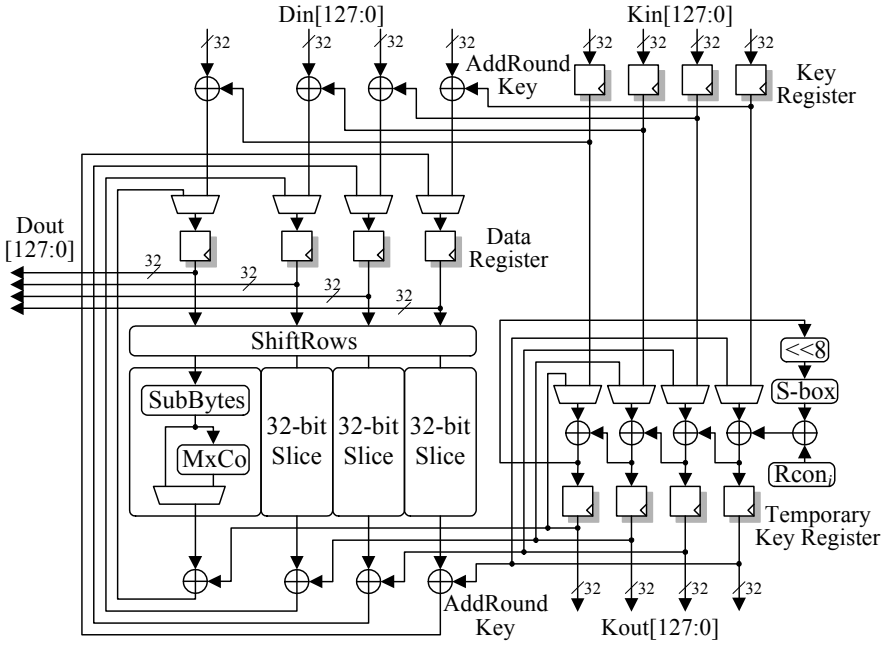



図 13-1　AES0 の暗号化処理のデータパス

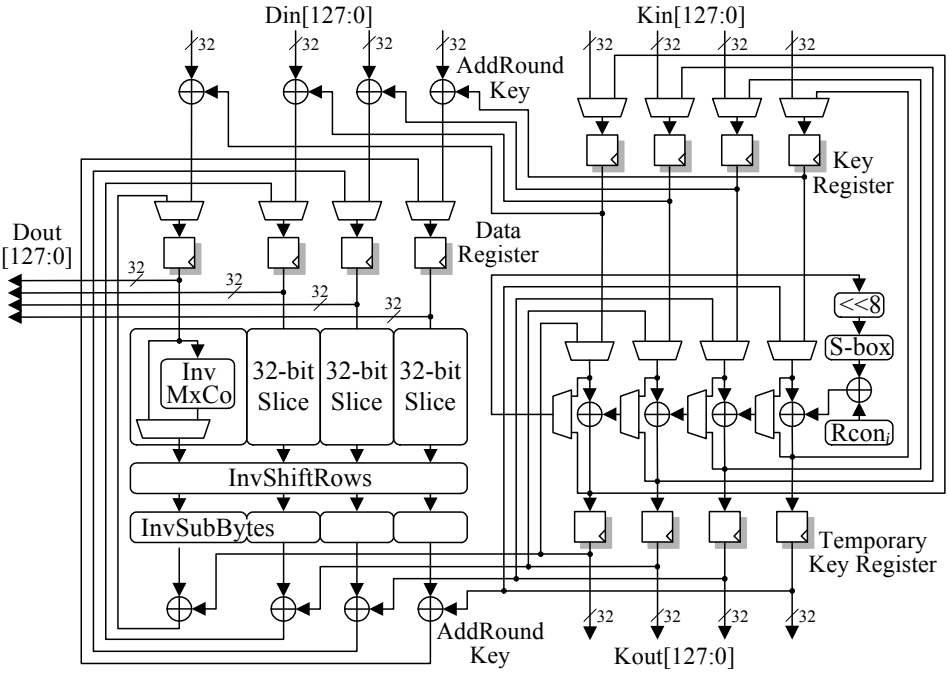



図 13-2　AES0 の復号処理のデータパス

図 13-3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.

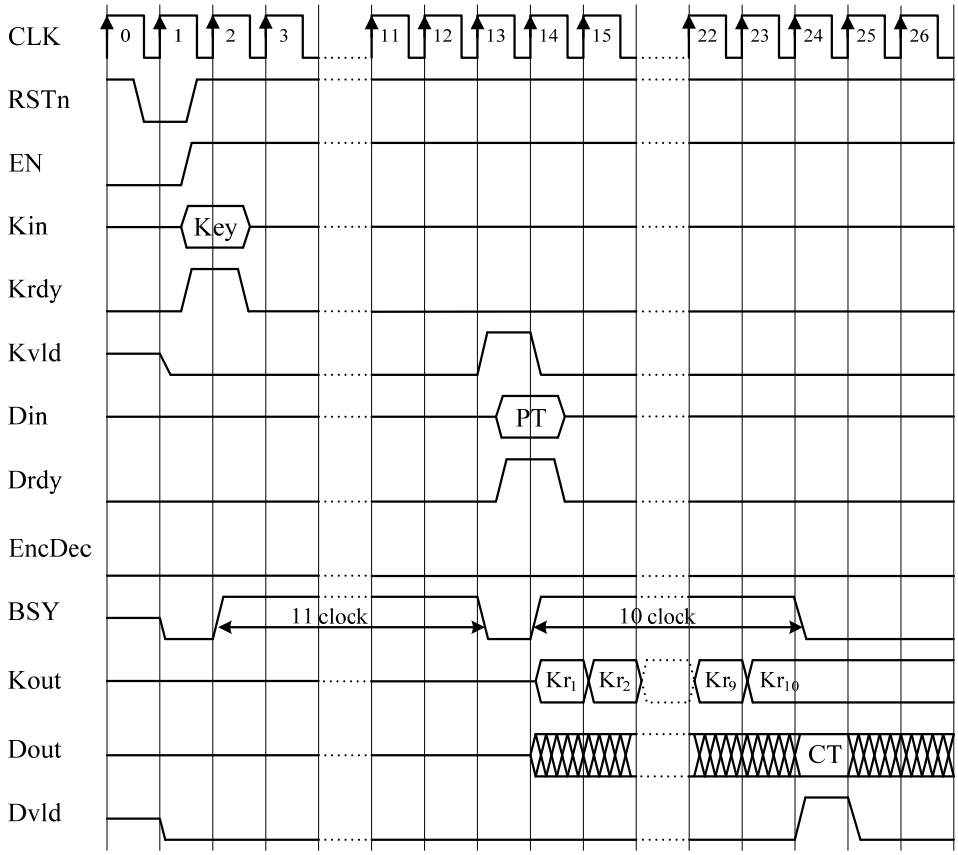



図 13-3　AES0 の暗号化処理のタイミングチャート

図 13-4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.

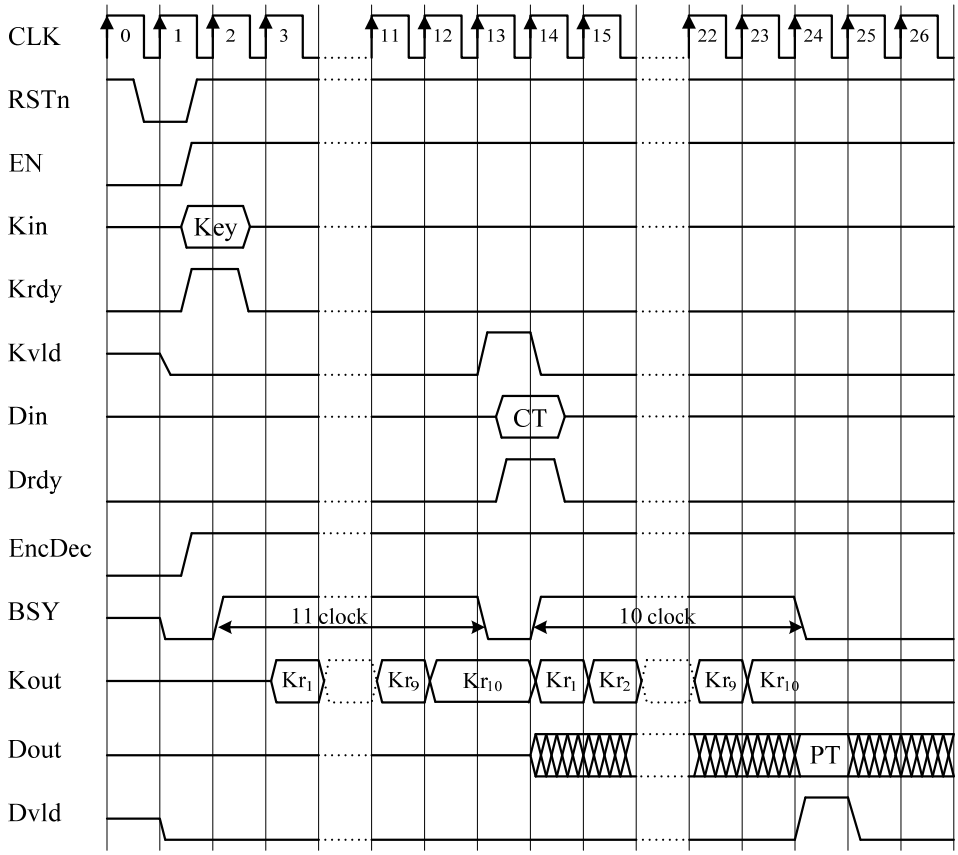



図 13-4　AES0 の復号処理のタイミングチャート

## 13.2. 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 13-3に，I/Oポートを表 13-4に示す．データパスアーキテクチャは図 13-1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 13-5で示すタイミングチャートが異なっている．

表 13-3　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<br>AES2: ASE_PPRM1.v<br>AES3: AES_PPRM3.v<br>AES4: AES_Comp.v |
| 記述言語 | Verilog-HDL |

| | |
|---|---|
| トップモジュール名 | AES1: AES_TBL<br>AES2: ASE_PPRM1<br>AES3: AES_PPRM3<br>AES4: AES_Comp |
| S-box | AES1: Look-up Table<br>AES2: PPRM1<br>AES3: PPRM3<br>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 13-4　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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

図 13-5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.

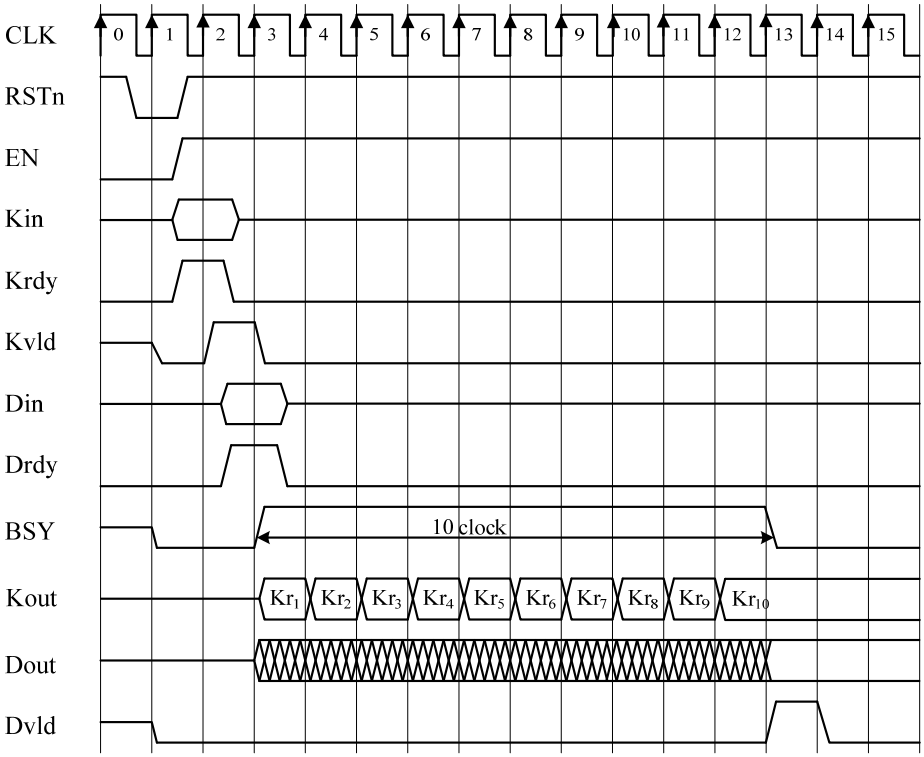



図 13-5　AES1/AES2/AES3/AES4 のタイミングチャート

## 13.3. 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 13-5表 13-5に, I/Oポートを表 13-6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. 従って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 13-5　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(((2$^2$)$^2$)$^2$) |
| スループット | 128 bits * 4 blocks / 46 clocks |
| ラウンド鍵生成 | On-the-fly |

表 13-6　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 Dvld=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 13-6図 13-6に示す. S-boxは合成体GF(((2²)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.

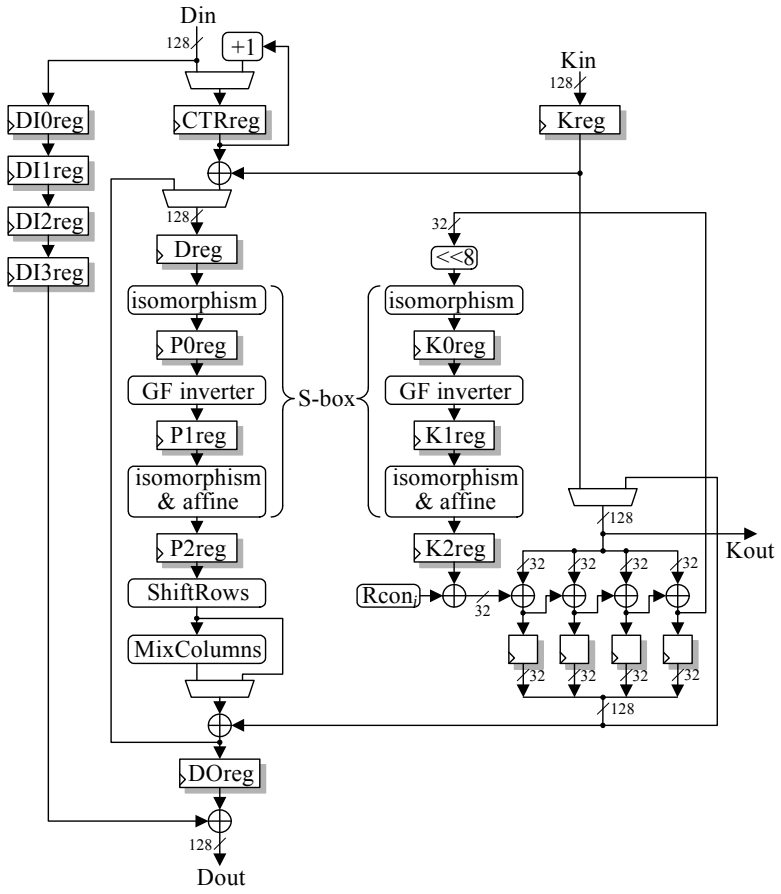



図 13-6　AES5 のデータパス

図 13-7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.

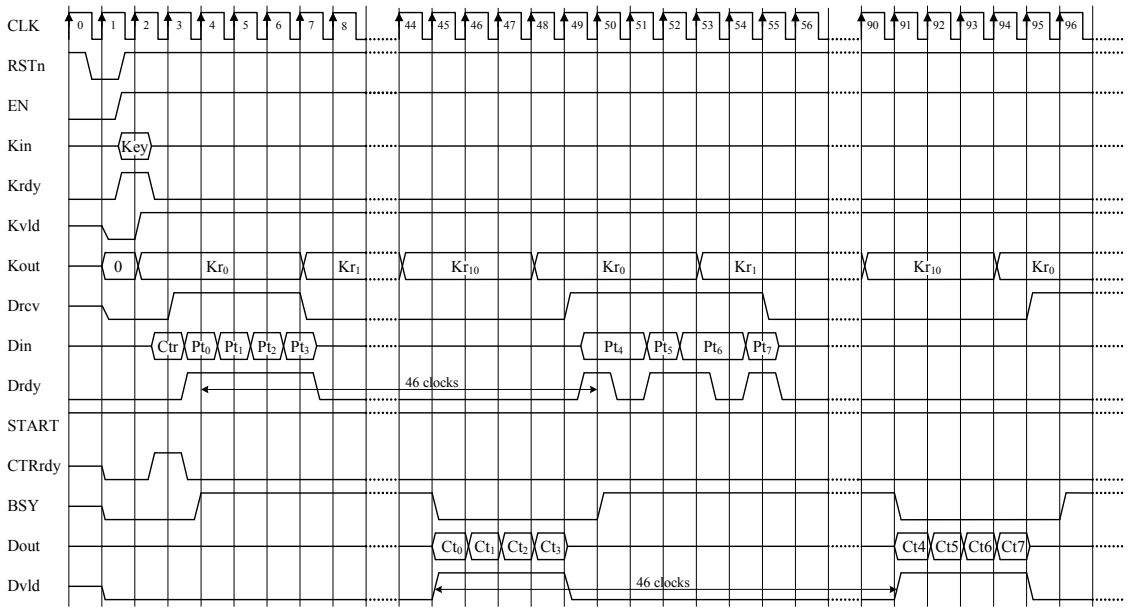



図 13-7-1　AES5 の暗号化・復号処理のタイミングチャート

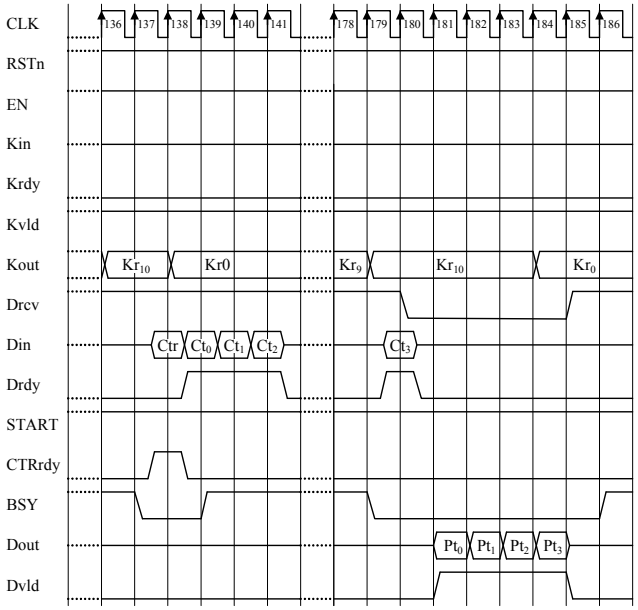



図 13-7-2　AES5 の暗号化・復号処理のタイミングチャート

図 13-8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 13-7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 13-7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．

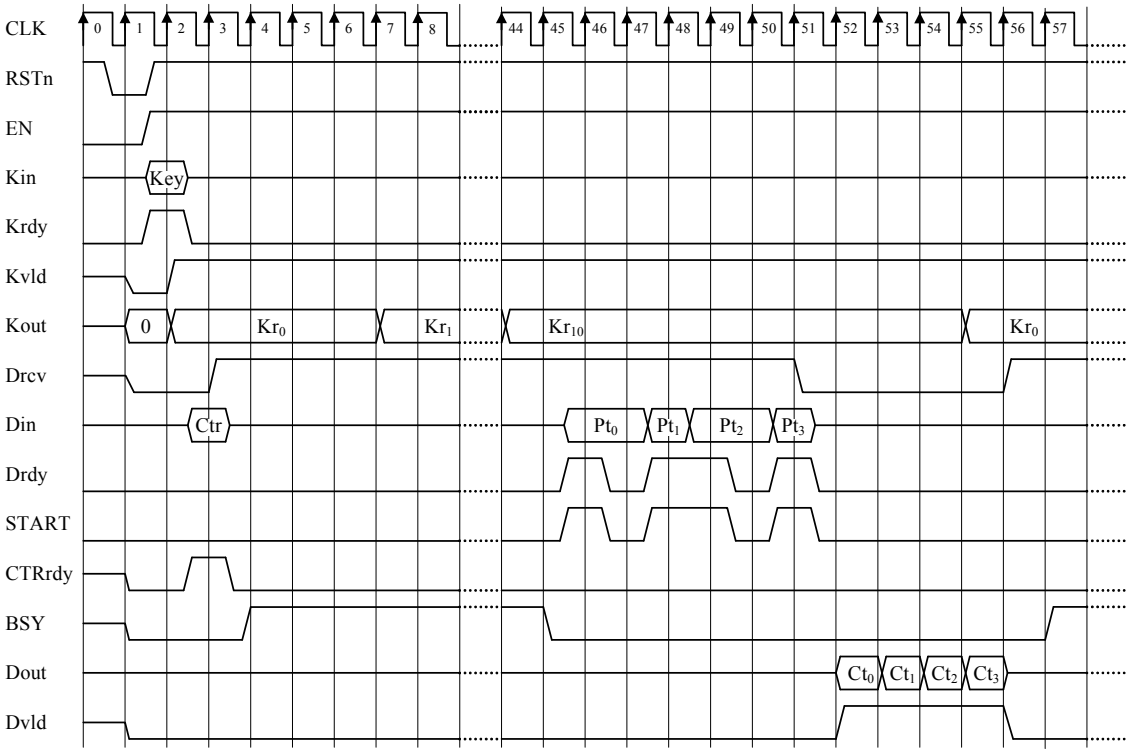



図 13-8-1　START 信号の制御を伴う AES5 のタイミングチャート

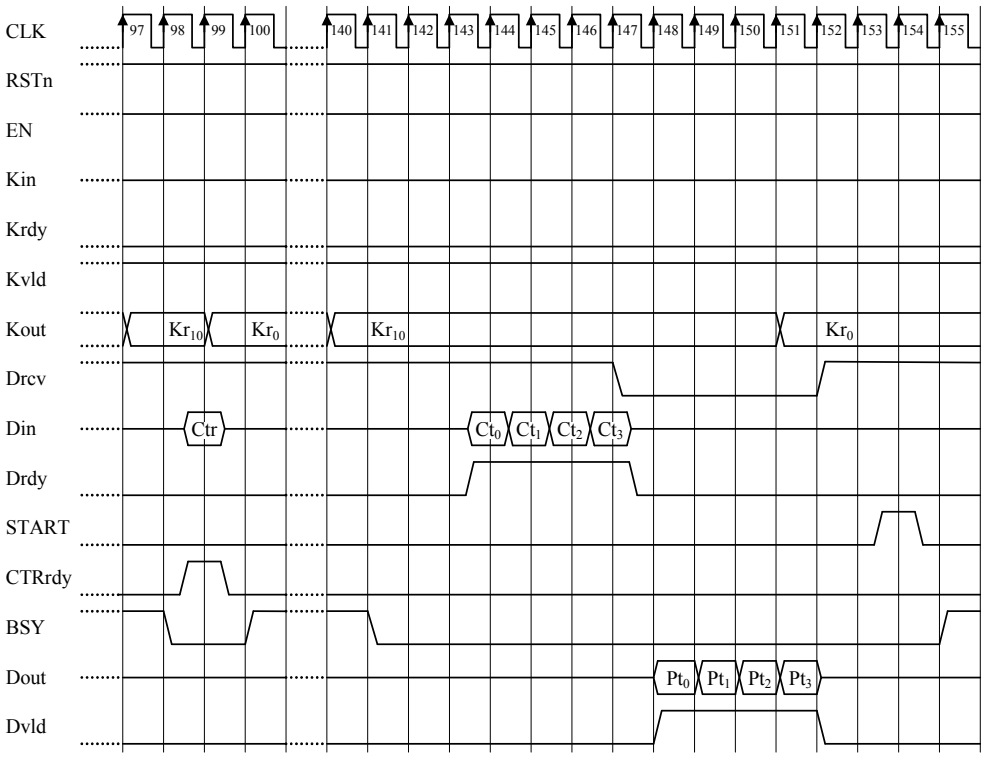



図 13-8-2　START 信号の制御を伴う AES5 のタイミングチャート

## 13.4. 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 13-7と表 13-8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 13-7　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 13-8　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 Dvld=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<br>=1: データエラー発生<br>Err[1]=0: 鍵エラーなし<br>=1 鍵エラー発生 |

図 13-9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 13-9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.

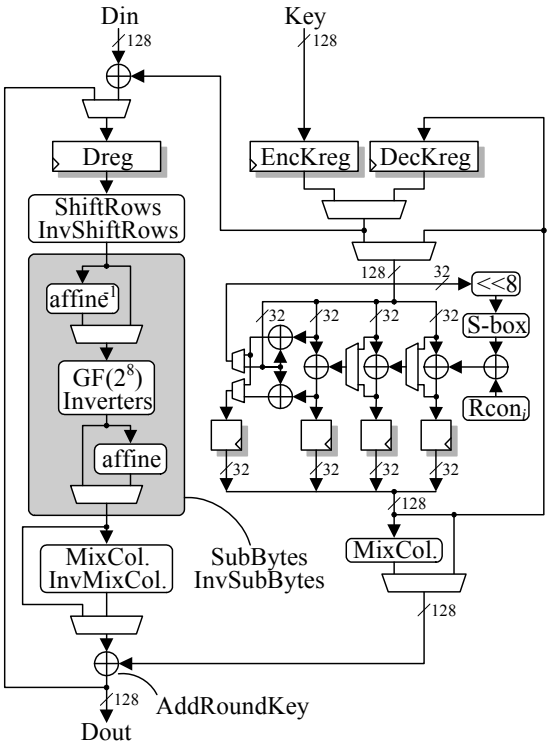



図 13-9　暗号化と復号でコンポーネントを共有する AES のデータパスアーキテクチャ

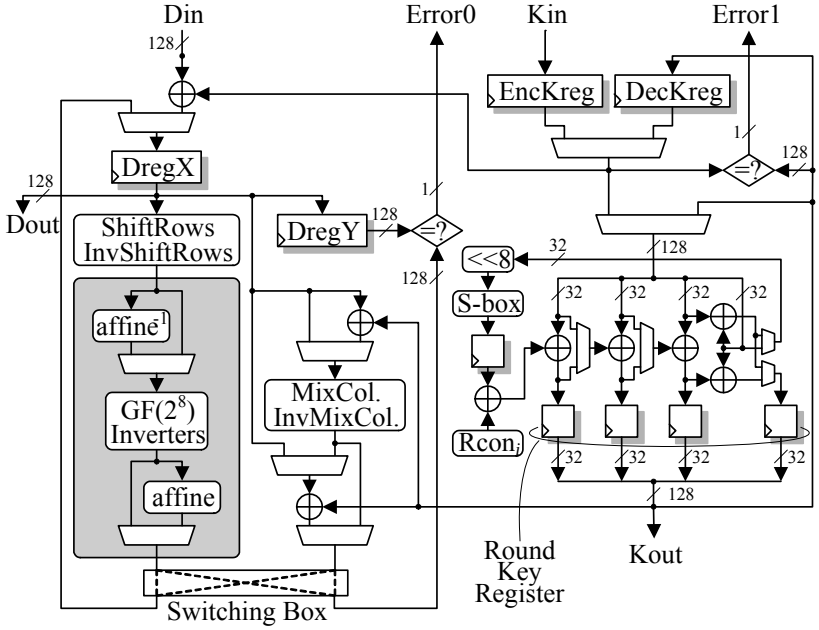



図 13-10　故障利用解析攻撃対策版 AES 暗号化・復号回路

図 13-10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 13-9図 13-9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 回で終了したりする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.

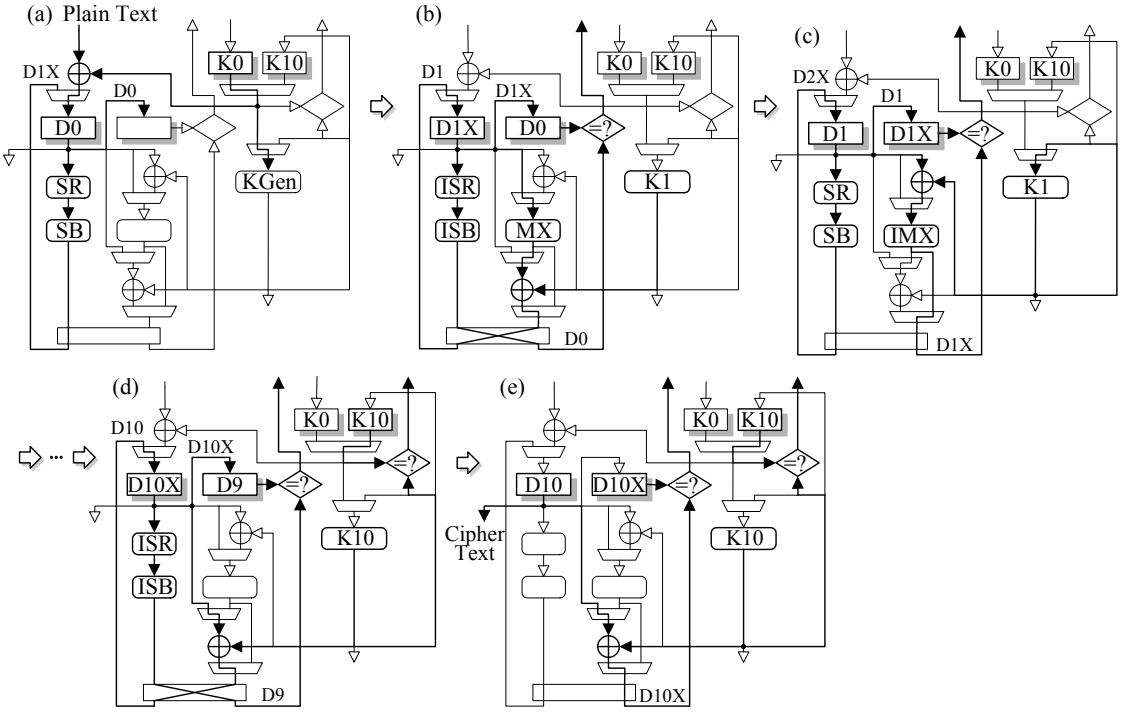



図 13-11　故障利用解析攻撃対策版回路の暗号化動作例

図 13-11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InvShiftRows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.

## 13.5. 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 13-9に, I/Oポートを表 13-10に示す.

表 13-9　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 13-10　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 Dvld=1 となり，次のクロックですぐに 0 に落とされる． |

図 13-12にAES7 のデータパスアーキテクチャを示す．図 13-1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．

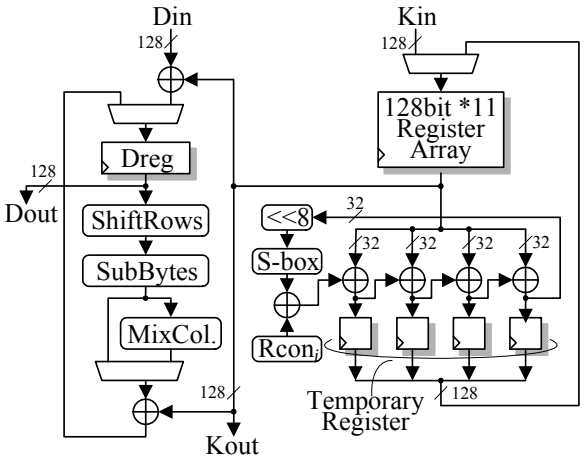



図 13-12　AES7 のデータパスアーキテクチャ

図 13-13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．

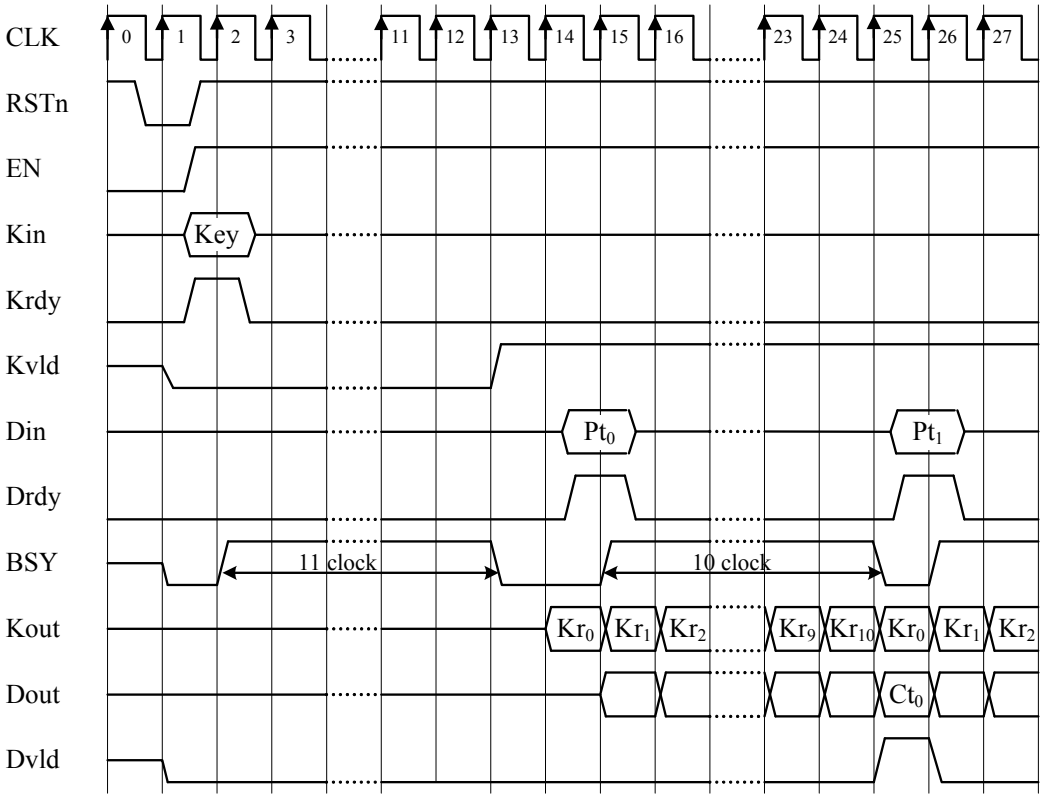



図 13-13　AES7 の暗号化のタイミングチャート

## 13.6. 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 13-14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.

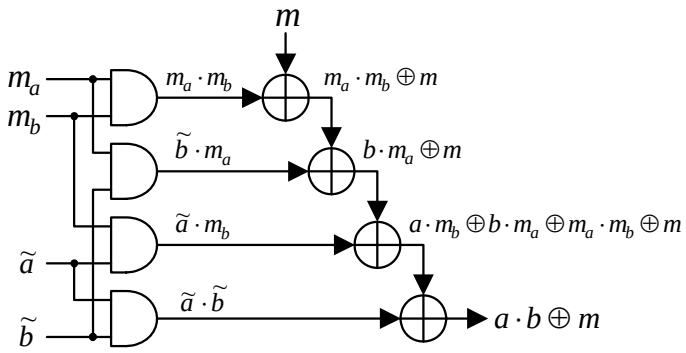



図 13-14　Masked-AND ゲート

## 13.7. 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13-15にMDPLの基本構成を示す．図13-15(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13-11に示す．

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

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13-15図13-15(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．

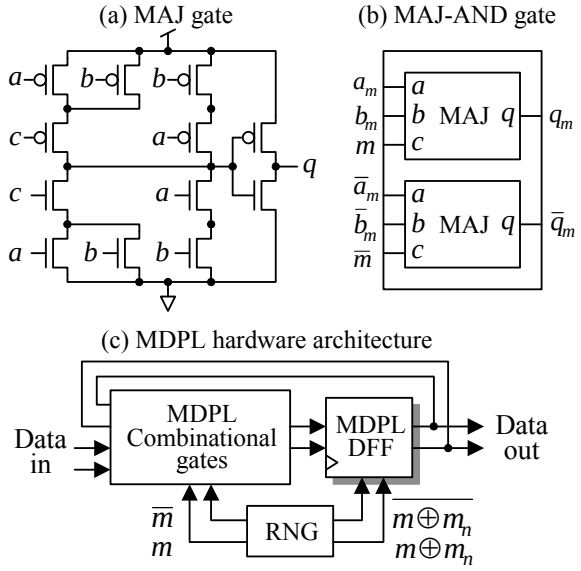



図 13-15　Masked Dual-rail Precharge Logic

表 13-11　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 |

## 13.8. 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$\oplus$，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．

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

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．

## 13.9. 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 13-16図 13-16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．

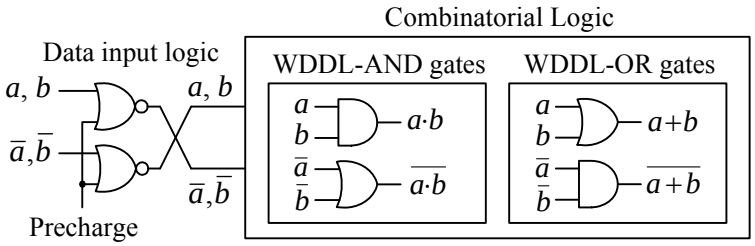



図 13-16　Wave Dynamic Differential Logic

## 13.10. 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13-17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: $\mathrm{RSL\text{-}NAND}(x_z, y_z, r_z, \overline{en})$ (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13-18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．

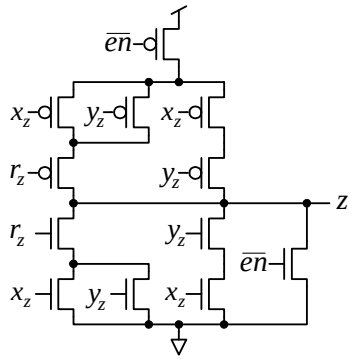



図 13-17　RSL-NAND ゲート

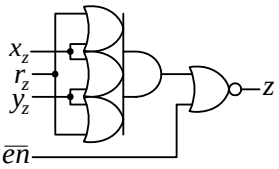



図 13-18　疑似 RSL-NAND ゲート

## 13.11. Camellia

Camellia[11] の暗号回路マクロ概要を表 13-12に，I/Oポートを表 13-13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 13-12　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 13-13　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 Dvld=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 13-19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.

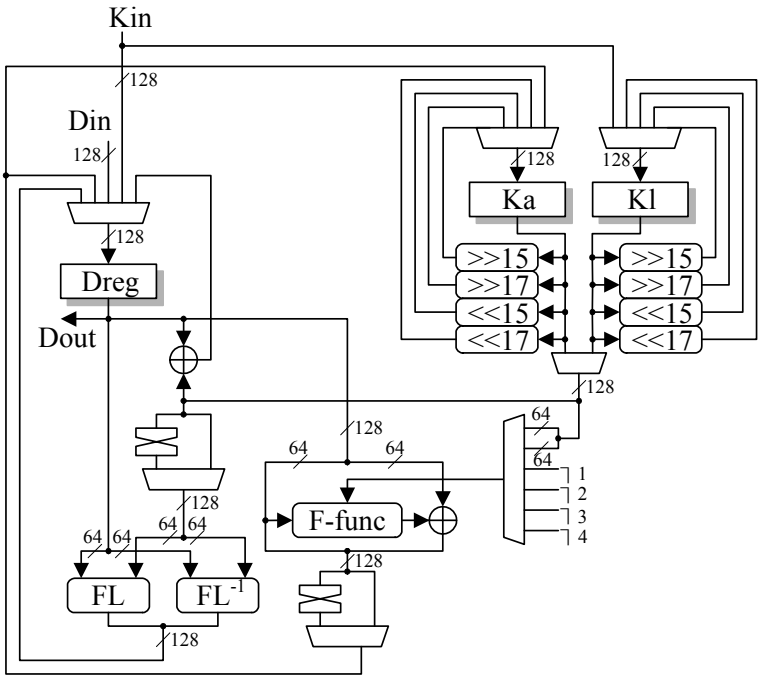



図 13-19　Camellia のデータパスアーキテクチャ

図 13-20に最短サイクルでの鍵スケジュールと暗号化, 図 13-21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.

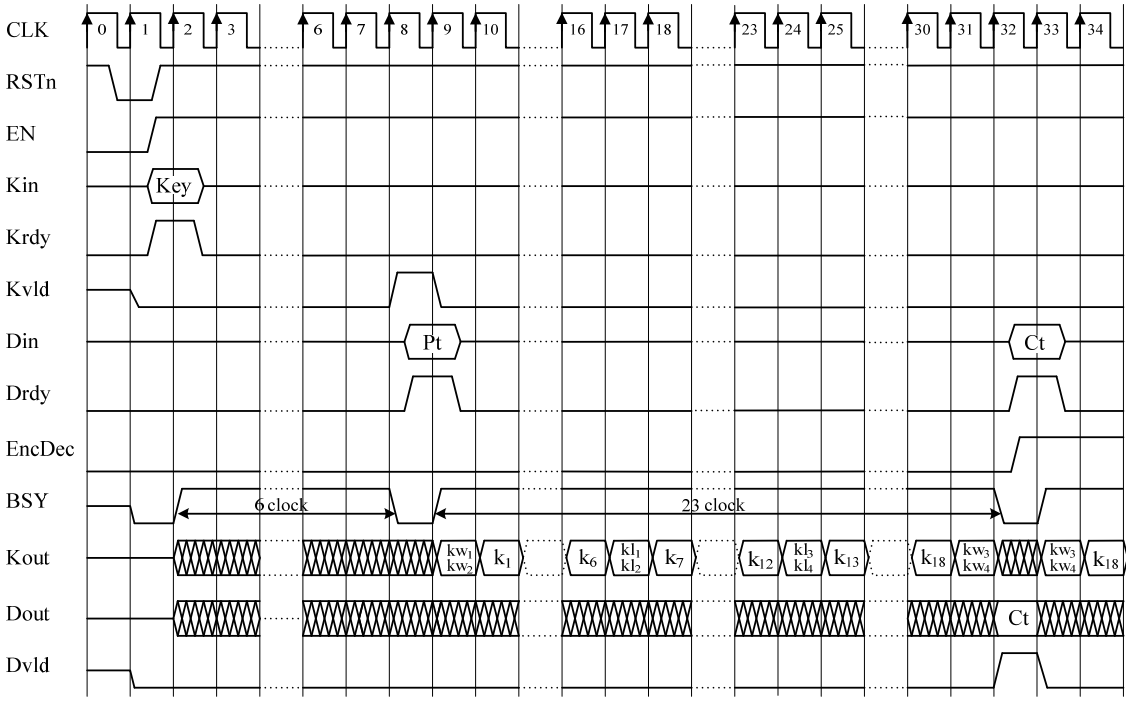



図 13-20　Camellia の鍵スケジュールと暗号化のタイミングチャート

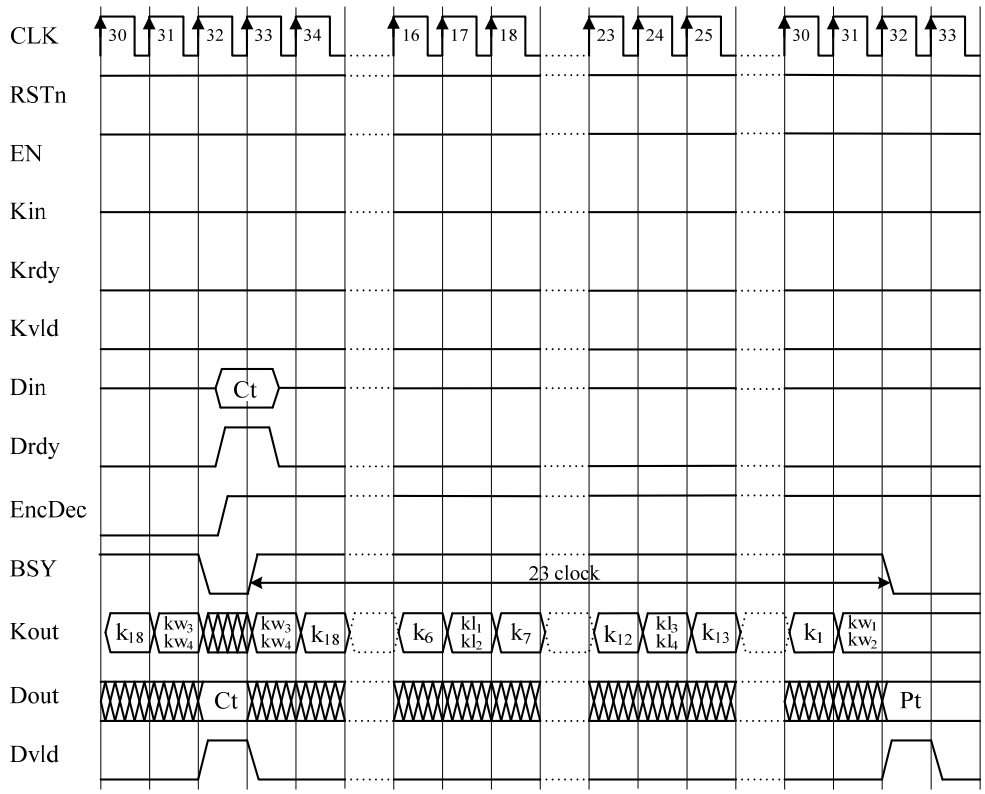



図 13-21　Camellia の復号タイミングチャート

## 13.12. 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 13-14に, I/Oポートを表 13-15に示す.

表 13-14　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 13-15　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 Dvld=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 13-22図 13-22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.

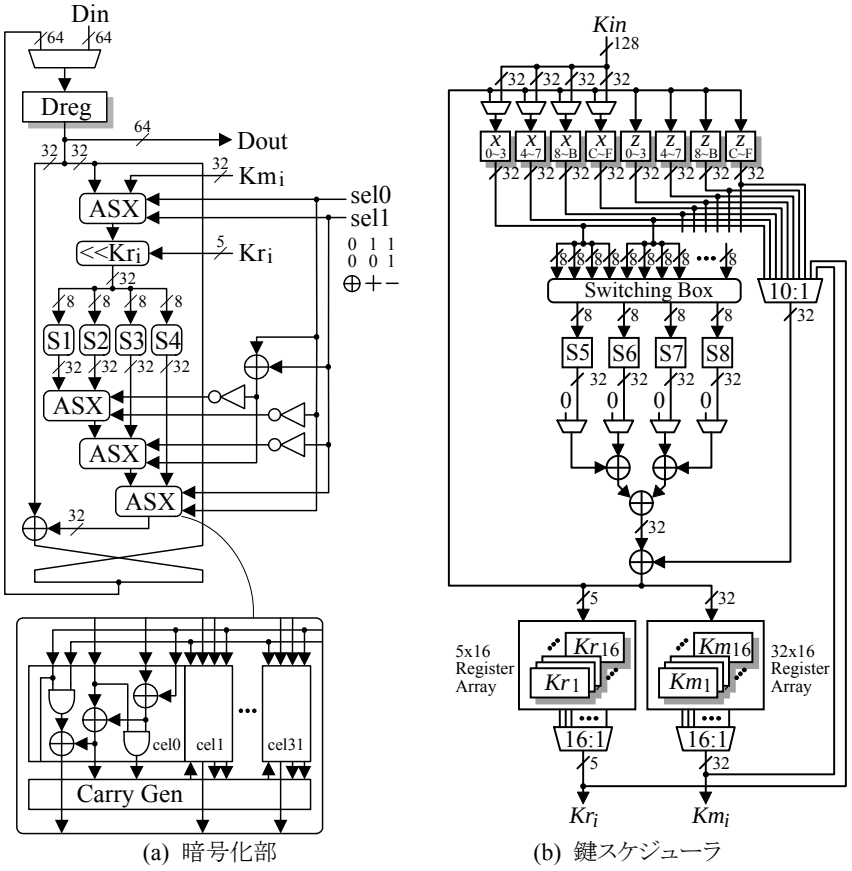



図 13-22　CAST-128 のデータパスアーキテクチャ

図 13-23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．

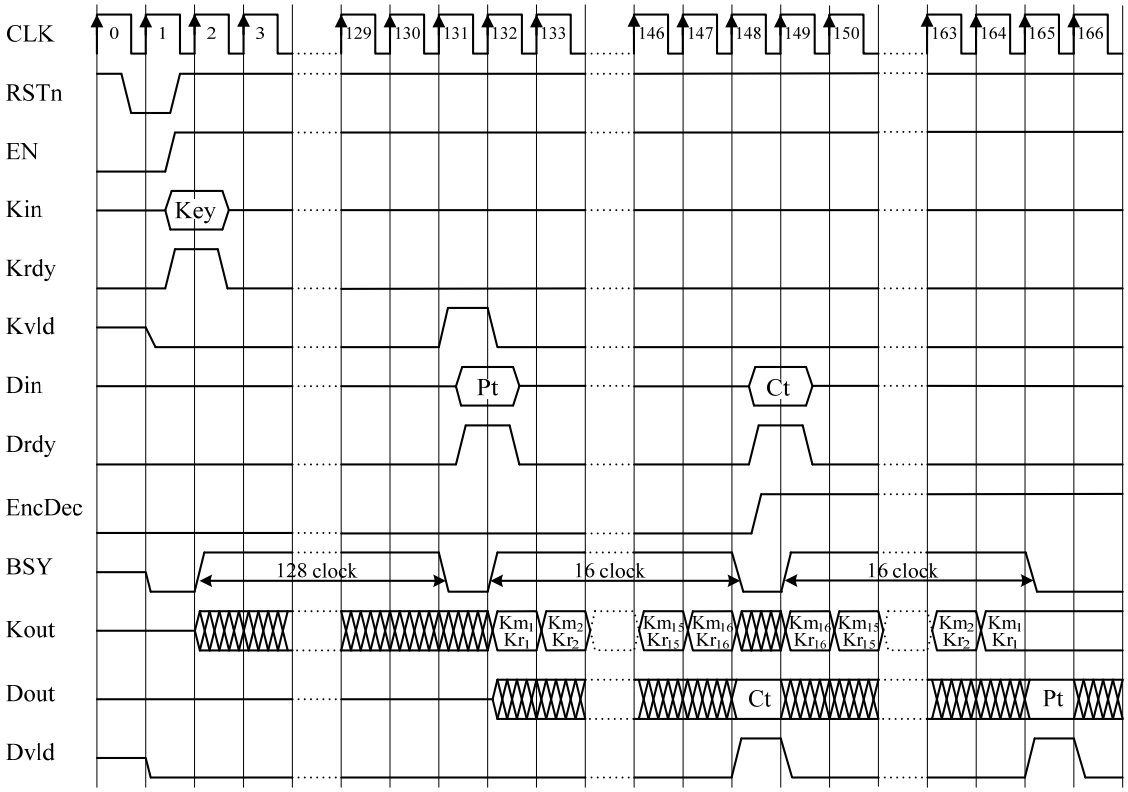



図 13-23　CAST-128 のタイミングチャート

## 13.13. DES

DES[14] の暗号回路マクロ概要を表 13-16に, I/Oポートを表 13-17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 13-16　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 13-17　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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

図 13-24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.

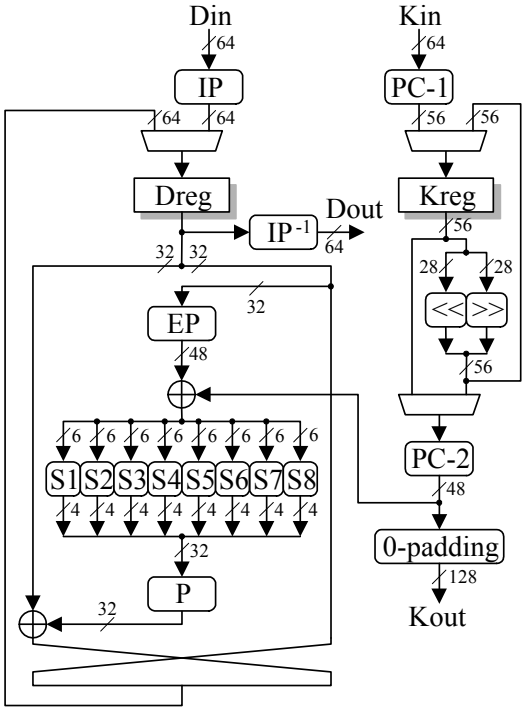



図 13-24　DES のデータパスアーキテクチャ

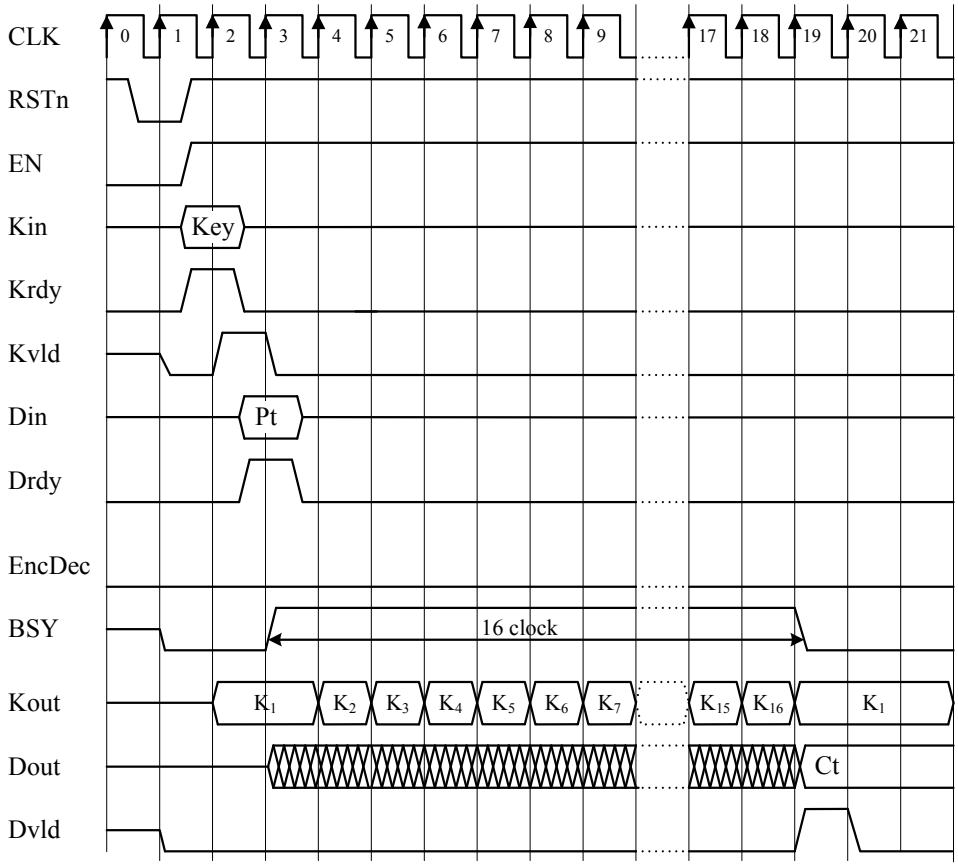



図 13-25　DES のタイミングチャート

図 13-25図 13-25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．

## 13.14. 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192bit×16wordのメモリマップをそれぞれ，表13-18～表13-20に示す．本マクロは既約多項式

$$f(x) = x^{191} + x^9 + 1$$

で定義される有限体GF($2^{191}$)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．ただし，鍵は64bitに制限している．

表 13-18　ECC 回路の概要

| | |
|---|---|
| アルゴリズム | データ値とアドレス値をランダム化可能な Montgomery Power Ladder 法 |
| データブロック長 | 192 bit |
| 鍵長 | 64 bit (制限付き) |
| 機能 | GF($2^{191}$)上の楕円スカラー倍算 |
| ソースファイル名 | uec_2nd_ECC_OS.v |
| 記述言語 | Verilog-HDL |
| トップモジュール名 | uec_2nd_ECC_OS |

表 13-19　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 64bit の乱数データの計 128bit を 32bit ずつ 4 クロックを用いたバースト転送で入力． |
| Din | In | 32 | 初期点等のデータ入力．192 ビットの Affine 座標系の初期点の x 座標，192 ビットの Projective 座標系の Z 座標(Z≠0)，192 ビットの楕円曲線パラメータ b の計 576 ビットを 32 ビットずつ 18 クロックを用いたバースト転送により入力． |
| Dout | Out | 32 | 楕円スカラー倍算計算結果出力．Dvld=1 が出力された後，192 ビットの楕円スカラー倍算結果の x 座標を出力データとして 32 ビットずつ 6 クロックを用いたバースト転送により出力． |

| | | | |
|---|---|---|---|
| Krdy | In | 1 | 1 クロックだけ Krdy=1 とすると，秘密鍵データと乱数データの計 128bit が 4 クロックを用いたバースト転送により Kin から入力され，内部レジスタに取り込まれる． |
| Drdy | In | 1 | 1 クロックだけ Drdy=1 とすると，192 ビットの Affine 座標系の初期点の x 座標，192 ビットの Projective 座標系の Z 座標(Z≠0)，192 ビットの楕円曲線パラメータ b が 18 クロックを用いたバースト転送により Din から入力され，内部レジスタに取り込まれる．その後，楕円スカラー倍算処理が開始される． |
| 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 ECC マクロがアクティブとなる．EN=0 のときは初期状態に戻る． |
| 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．スカラー倍算処理中，もしくはデータ取り込み中に 1 となる． |
| Kvld | Out | 1 | 鍵の入力が完了すると，1 クロックの間だけ Kvld=1 となる． |
| Dvld | Out | 1 | 初期点が取り込まれたときに 1 クロックだけ High となる． |

表 13-20　ECC 回路のメモリマップ

| アドレス | 用途 | アドレス | 用途 |
|---|---|---|---|
| 0 | 0 | 8 | $Z_2$ |
| 1 | 予約 | 9 | $Z_0$ |
| 2 | $R^2 \bmod M(x)$ = 0x402 | A | $Z_1$ |
| 3 | $x$ | B | 1 |
| 4 | $b$ | C | $X_2$ |
| 5 | $t_1$ | D | $X_0$ |
| 6 | $t_2$ | E | $X_1$ |
| 7 | $t_3$ | F | 予約 |

スカラー倍算アルゴリズムは射影座標上のMontgomery powering ladder法[15] であるLópez と Dahab のアルゴリズム[16] に対して，アドレス値をランダム化した伊藤らのアルゴリズム[17] の改良版を用いた．射影座標のZ座標に乱数を入力することでデータのランダム化を行うことができる．これらのアルゴリズムをそれぞれAlgorithm 1, 2, 3 に示す．また，データは全て多項式表記である．

● Algorithm 1: Montgomery Powering Ladder 法

入力:楕円曲線上の点 $P$, 正の整数 $d = (1d_{k-2}\cdots d_1 d_0)_2$

出力:$dP$ の x 座標 $x(dP)$

1: $P_1 \leftarrow P, P_2 \leftarrow 2P$
2: **for** $i$=$k$-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** $x(P_1)$

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

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

出力: $P_1 = P_1 + P_2$

1: $X_1 \leftarrow X_1 Z_2$
2: $Z_1 \leftarrow X_2 Z_1$
3: $t_1 \leftarrow X_1 Z_1$
4: $Z_1 \leftarrow X_1 + Z_1$
5: $Z_1 \leftarrow Z_1 Z_1$
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: $t_2 \leftarrow X_1 X_1$
2: $t_3 \leftarrow Z_1 Z_1$
3: $Z_1 \leftarrow t_2 t_3$
4: $t_2 \leftarrow t_2 t_2$
5: $t_3 \leftarrow t_3 t_3$
6: $X_1 \leftarrow bt_3 + t_2$
7: **return** $P_1$

● Algorithm 3: アドレス値をランダム化した Montgomery powering ladder 法.

入力: $P$, $k = (1, k_{n-2}, \cdots, k_0)_2$, $r = (r_{n-2}, \cdots, r_0)_2$

出力: $x(kP)$

1: $\mathrm{R}[r_{n-1}] \leftarrow x(2P)$
2: $\mathrm{R}[1 \oplus r_{n-1}] \leftarrow x(P)$
3: **for** $i$ = $n$-2 **downto** 0 **do**
4: $\mathrm{R}[2] \leftarrow \mathrm{PD}(\mathrm{R}[k_{i+1} \oplus k_i \oplus r_{i+1}])$
5: $\mathrm{R}[1 \oplus r_i] \leftarrow \mathrm{PA}(\mathrm{R}[0], \mathrm{R}[1])$
6: $\mathrm{R}[r_i] \leftarrow \mathrm{R}[2])$
7: **end for**
8: **return** $\mathrm{R}[k_0 \oplus r_0]$

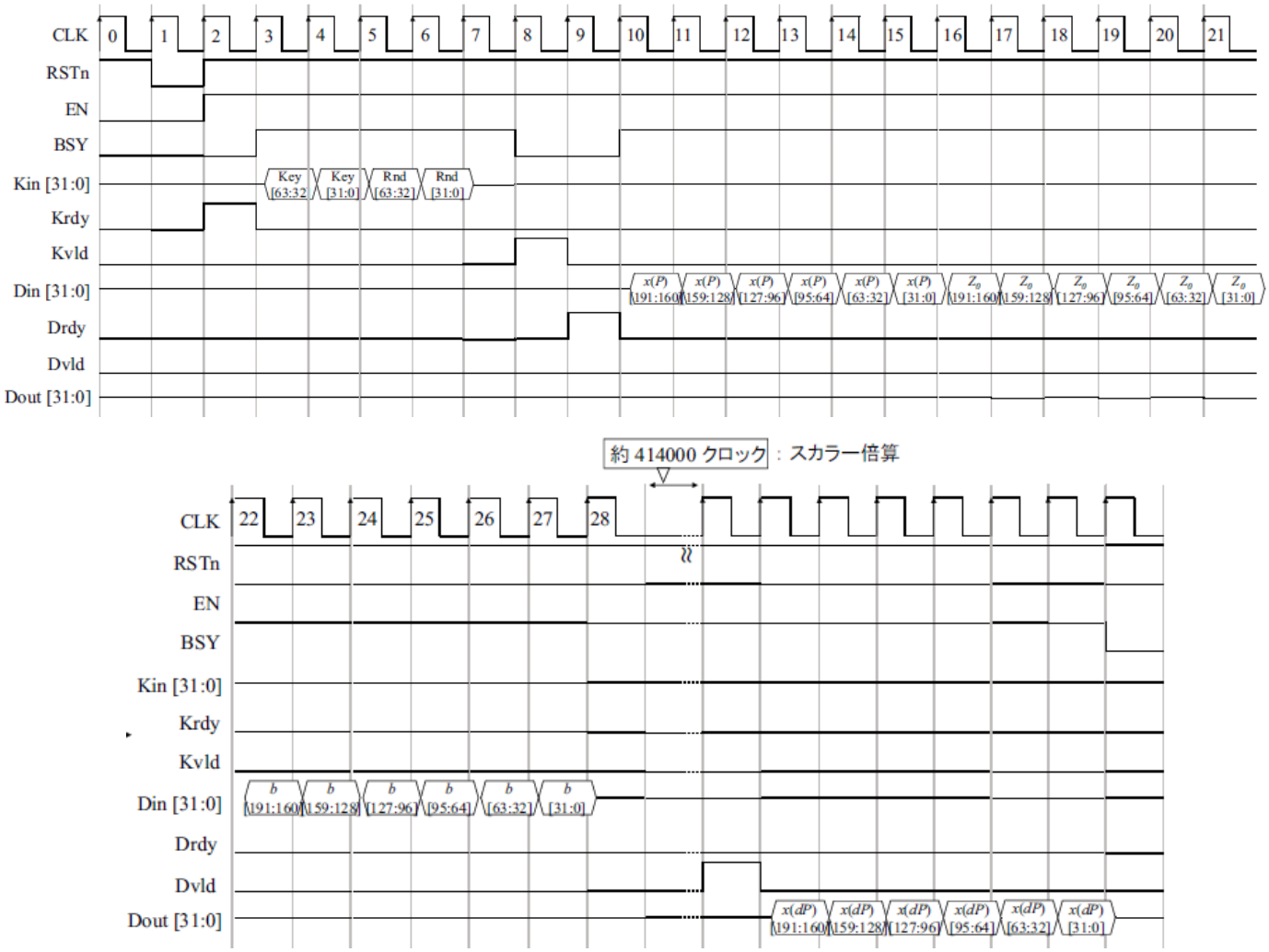



図 13-26　ECC のタイミングチャート

図 13-26に本ECC回路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:** 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．

**CLK3~8:** 64 bits の鍵データと乱数データを 32 bits ずつ 4 クロックを用いたバースト転送によって取り込み，それぞれ内部の鍵レジスタ，乱数レジスタにそれぞれ格納する．データ格納後，すなわち **CLK8** で 1 クロックの間だけ Kvld=1 が出力される．またビジーフラグ BSY=1 となる．

**CLK9~27:** CLK9 で初期点等のデータを取り込むために Drdy=1 とする．Affine 座標系で表された初期点の x 座標成分である 192 bits の x と射影座標で表された 192 bits の Z 座標($Z \neq 0$) および 192bits の楕円曲線パラメータ b をそれぞれ 32 bits ずつ 18 クロックを用いたバースト転送によって取り込み，内部メモリにそれぞれ格納する．

**CLK28~:** 約 414000 クロックかけて楕円スカラー倍算処理を行う．処理が終わると 1 クロックの間だけ Dvld=1 となり，その後 192 bits の楕円スカラー倍算結果が 32 bits ずつ 6 クロックを用いてバースト転送により出力される．

## 13.15. MISTY1

MSITY1[18] の暗号回路マクロ概要を表 13-21に, I/Oポートを表 13-22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 13-21　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 13-22　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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

図 13-27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.

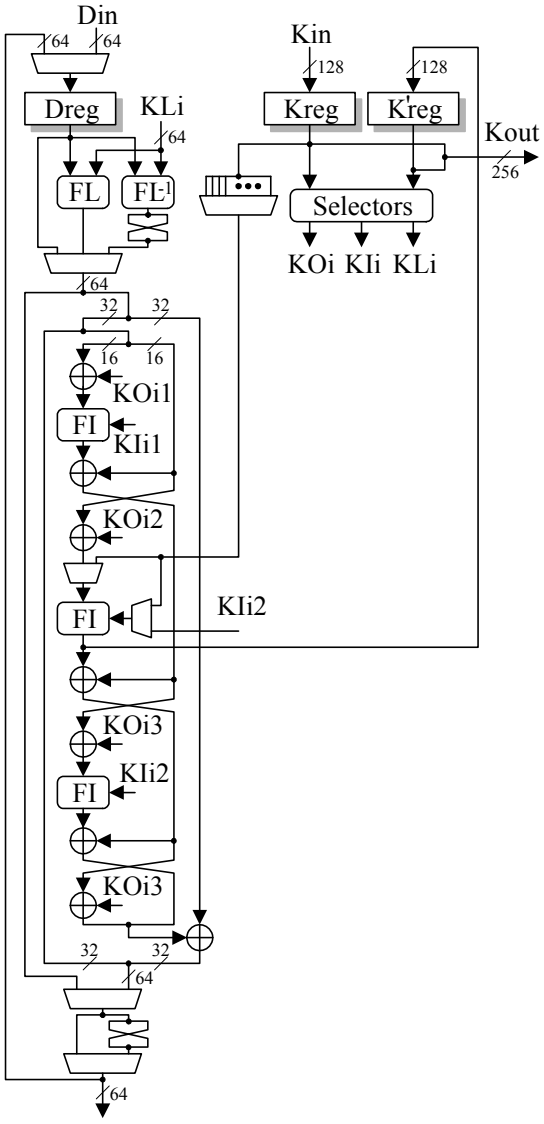



図 13-27　MISTY1 のデータパスアーキテクチャ

図 13-28図 13-28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 Kreg 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:** EncDec=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.

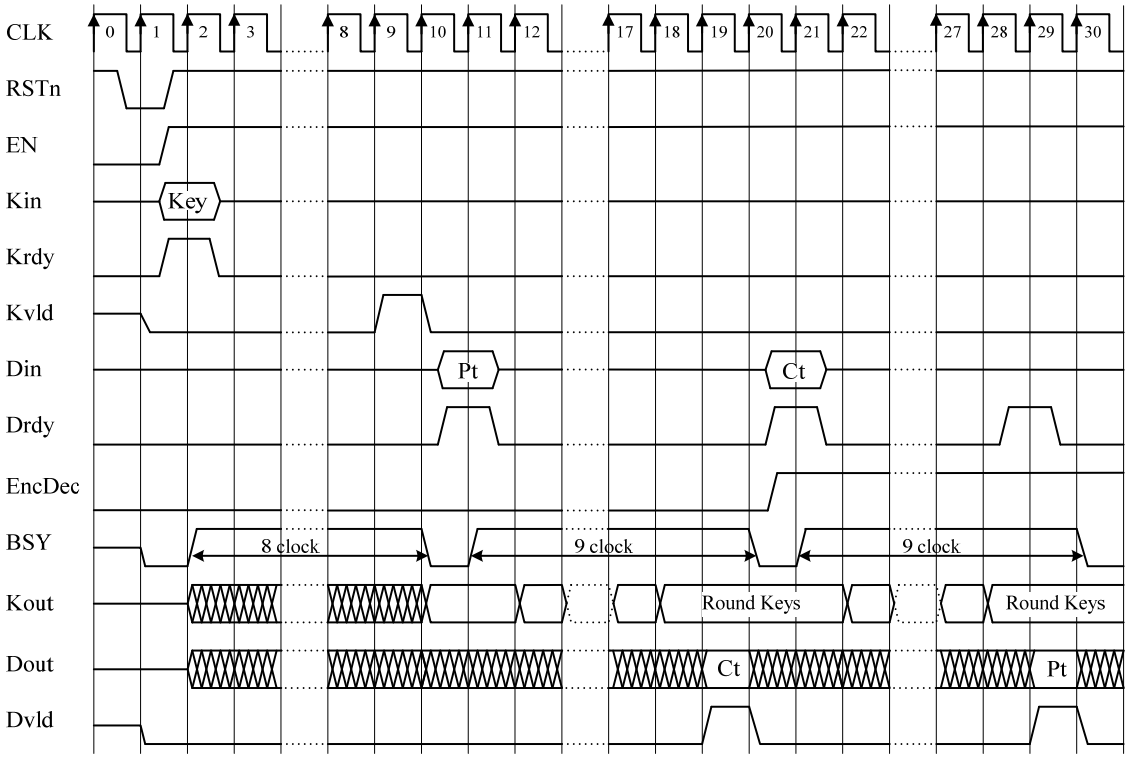



図 13-28　MISTY1 のタイミングチャート

## 13.16. RSA

RSAの暗号回路マクロ概要を表 13-23に, I/Oポートを表 13-24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] および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 13-23　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)<br>べき乗剰余演算<br>0)左バイナリ法<br>1) 右バイナリ法<br>2) 左バイナリ法+ダミー乗算<br>3) 右バイナリ法+ダミー乗算<br>4) Montgomery Powering Ladder<br>5) Square-Multiply べき乗法 |
| 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<br>512 bit / 約 452K clocks – 0) 1)<br>512 bit / 約 599K clocks – 2) 3) 4) 5)<br>CRT<br>512 bit / 約 135K clocks – 0) 1)<br>512 bit / 約 176K clocks – 2) 3) 4) 5) |

表 13-24　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. |

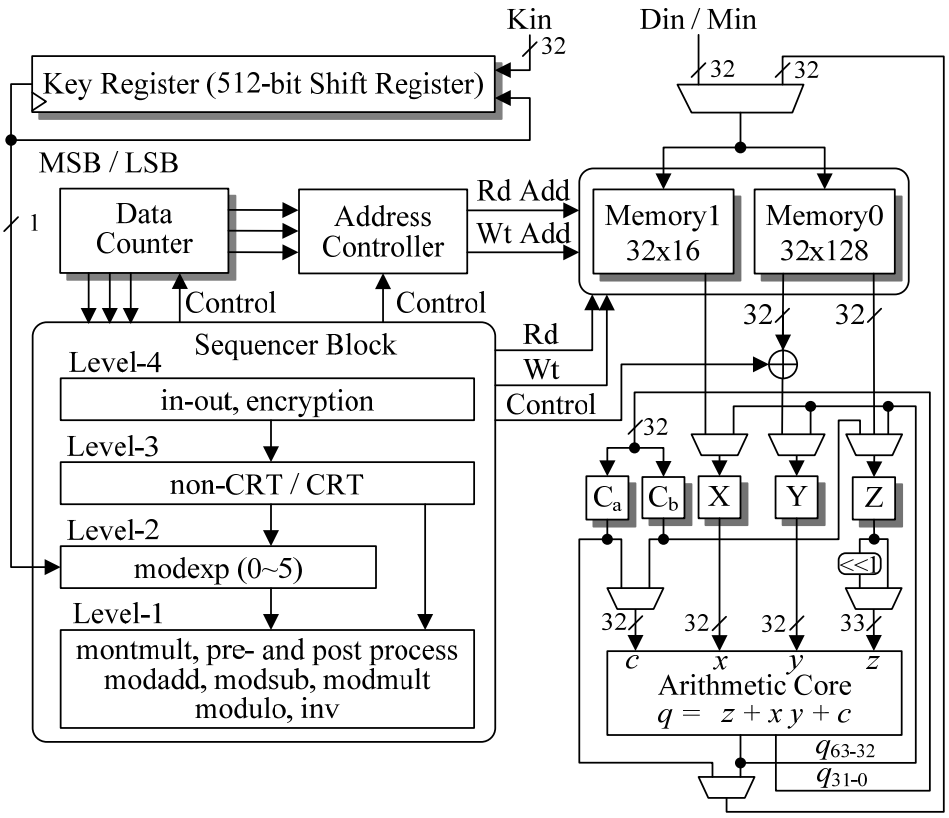



図 13-29　RSA 暗号マクロの回路アーキテクチャ

図 13-29図 13-29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 13-30図 13-30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.

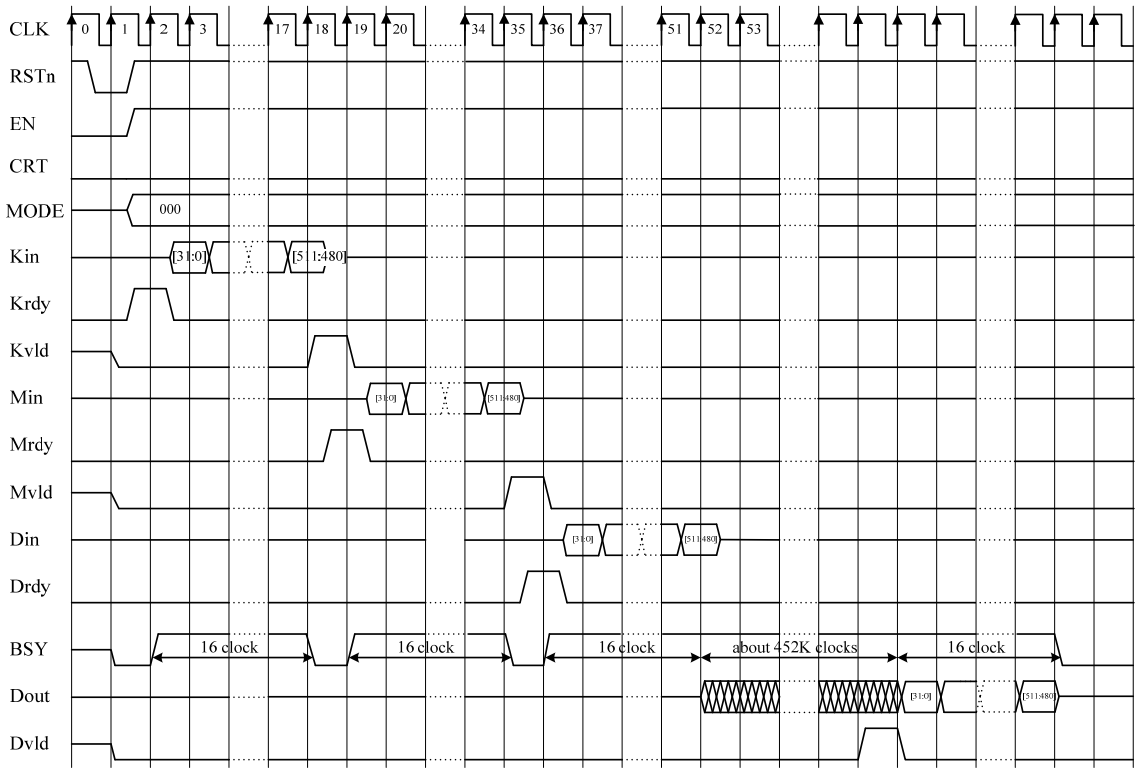



図 13-30　RSA のタイミングチャート(non-CRT)

**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 13-31図 13-31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 13-30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．

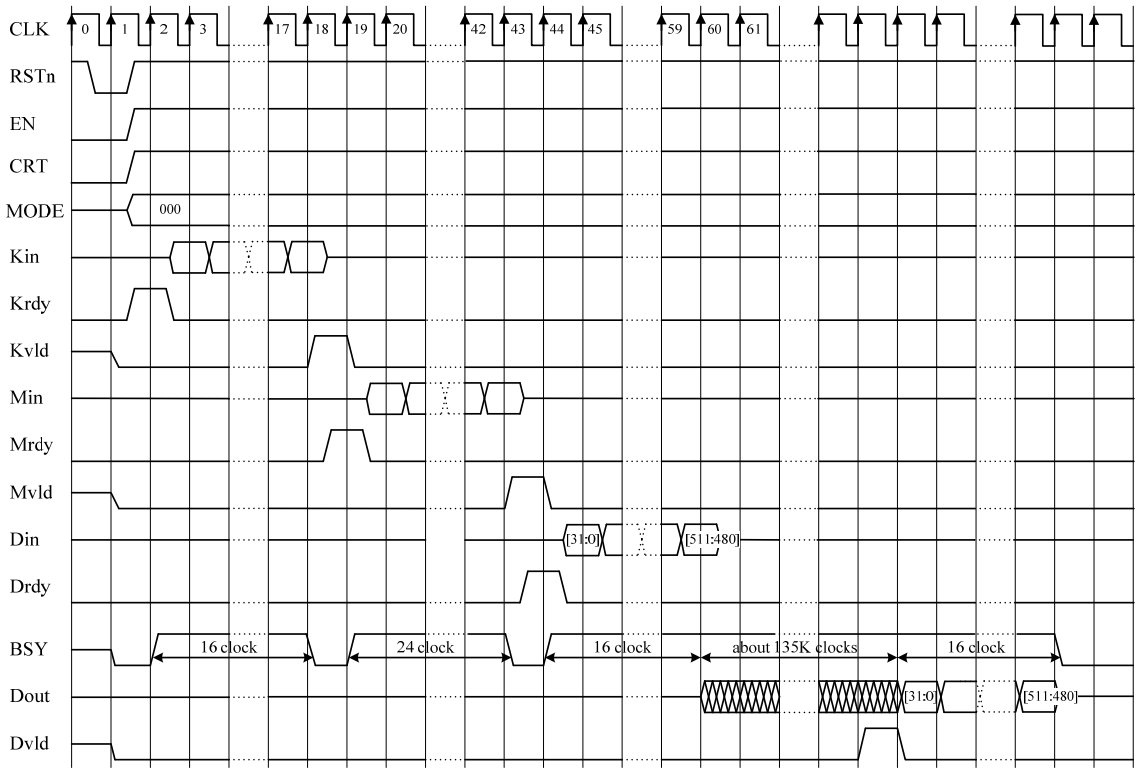



図 13-31　RSA のタイミングチャート(CRT)

## 13.17. SEED

SEED[26] の暗号回路マクロ概要を表 13-25に, I/Oポートを表 13-26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 13-25　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 13-26　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 Dvld=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 13-32図 13-32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.

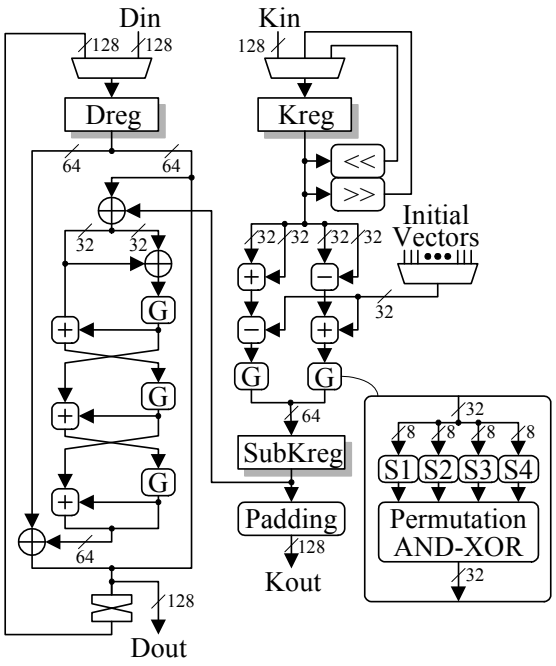



図 13-32　SEED のデータパスアーキテクチャ

図 13-33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．

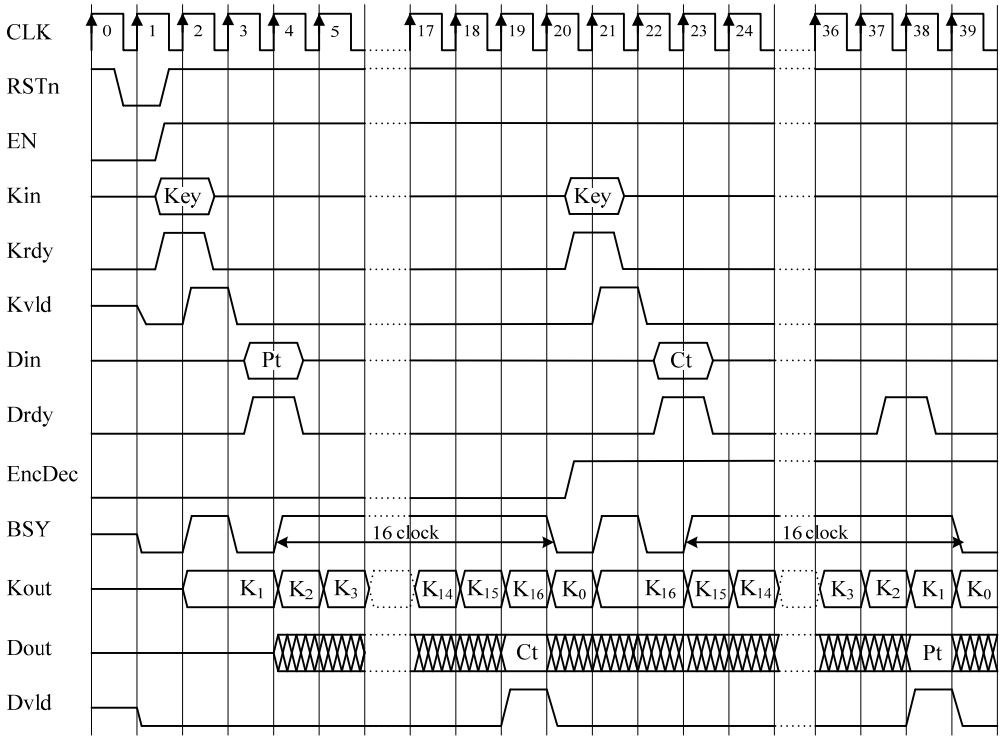



図 13-33　SEED のタイミングチャート

## 13.18. TDES

TDES (Triple-DES)[14] の暗号回路マクロ概要を表 13-27に, I/Oポートを表 13-28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複号では「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 13-27　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 13-28　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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

図 13-34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.

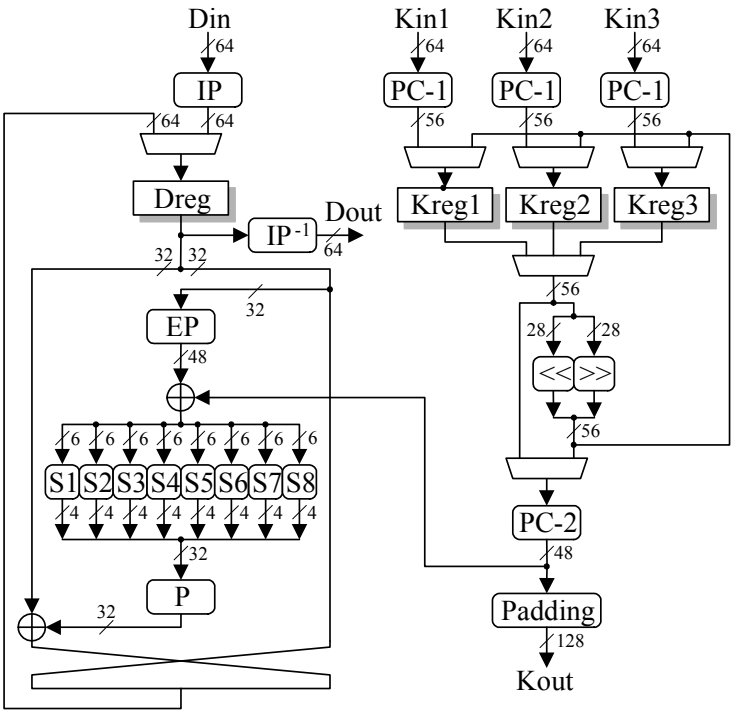



図 13-34　TDES のデータパスアーキテクチャ

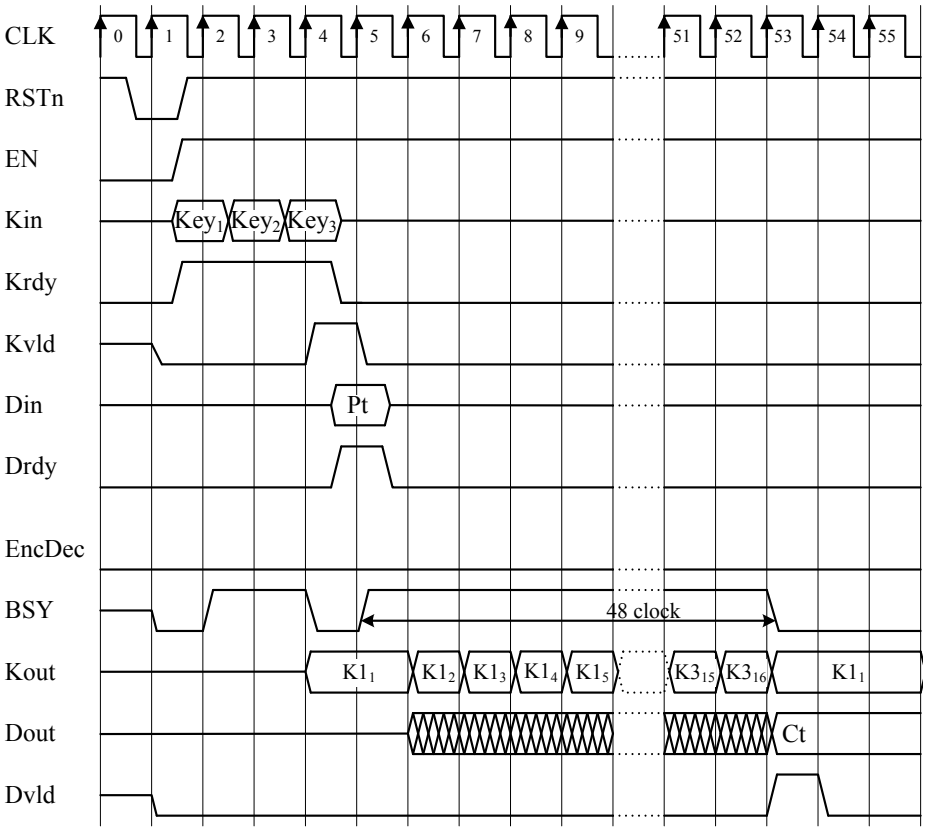



図 13-35　TDES のタイミングチャート

図 13-35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.

## 13.19. CLEFIA

CLEFIA[27), 28)] の暗号回路マクロ概要を表 13-29に, I/Oポートを表 13-30に示す. CLEFIAは SONYが開発したブロック長 128 ビットのブロック暗号であり, 鍵長は 128, 192, 256 ビットがサポートされている. 本マクロでは, ECB (Electronic Code Book) モードのみがサポートされているが, CBC (Cipher Block Chaining) 等の他のモードも, バッファや制御回路を追加することで容易に構成可能である. なお, 本マクロは文献[29)]を参考に作成された.

表 13-29 CLEFIA の概要

| | |
|---|---|
| アルゴリズム | CLEFIA |
| データブロック長 | 128 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 | CLEFIA_Comp.v |
| 記述言語 | Verilog-HDL |
| トップモジュール名 | CLEFIA_Comp |
| スループット | 128 bit / 18 clock (暗号化)<br>128 bit / 19 clock (復号) |
| ラウンド鍵生成 | On-the-fly |

表 13-30 CLEFIA の I/O ポート

| ポート名 | 方向 | ビット幅 | 説明 |
|---|---|---|---|
| Kin | In | 128 | 鍵入力. |
| 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 CLEFIA 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 Dvld=1 となり, 次のクロックですぐに 0 に落とされる. |

図 13-36にCLEFIA回路のデータパスアーキテクチャを示す. このマクロは, Generalized Feistel Network (GFN) の 1 ラウンドを 1 クロックサイクルで実行する. 1 ブロックの暗号化には 18 サイクル, 復号には 19 サイクルを要する. 秘密鍵は 128 ビットのKinポートから入力され, 内部レジスタKに保持される. その後, データランダム化部において鍵初期化処理が 13 サイクルかけて行われ, 中間鍵がレジスタLに格納される. 暗号化/復号処理の間, ラウンド鍵はレジスタKおよびLに格納されたデータを用いてon-the-flyで生成される. 入力データ(平文または暗号文)は 128 ビットのDinポートから入力され, 内部レジスタに保持される. 出力データ(暗号文または平文)は 128 ビットのDoutポートから出力される.

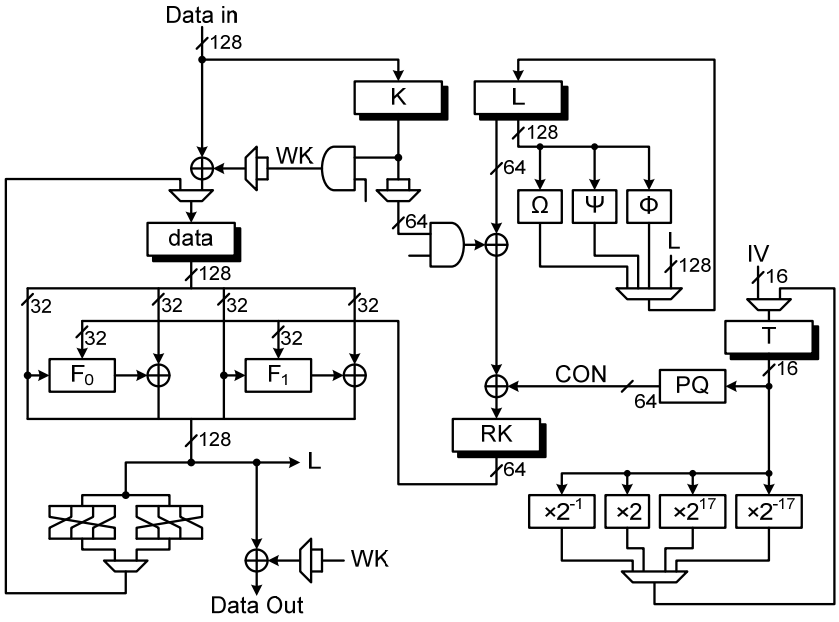



図 13-36　CLEFIA のデータパスアーキテクチャ

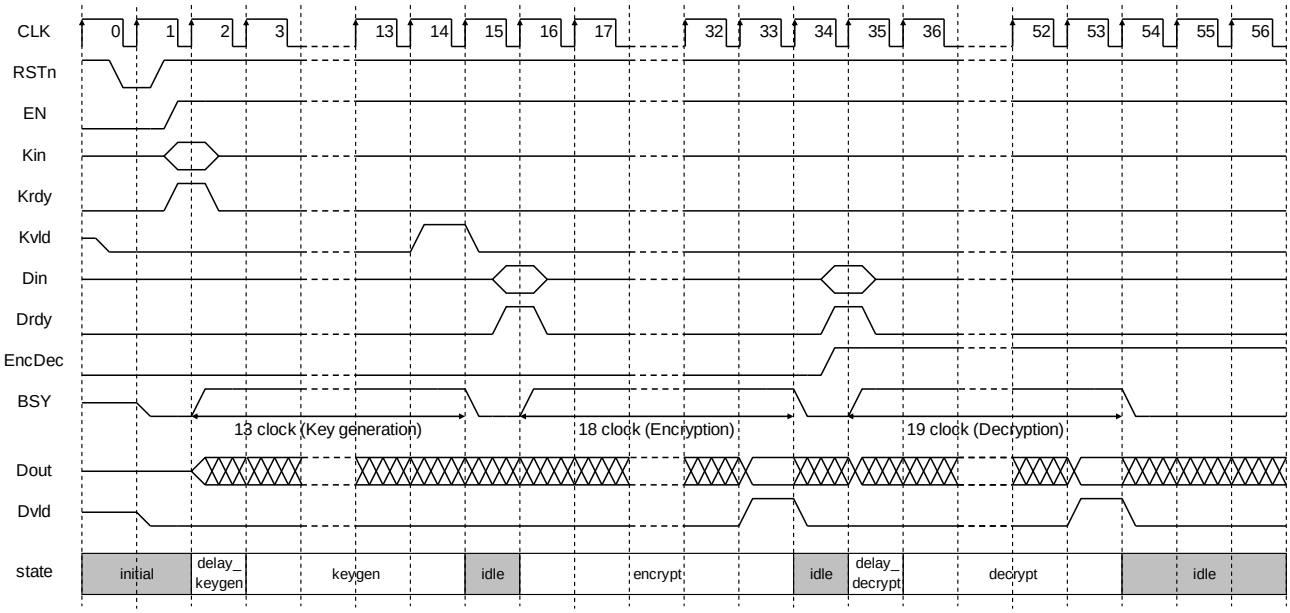



図 13-37　CLEFIA のタイミングチャート

図 13-37図 13-37に, 最短サイクルでのCLEFIAの暗号化処理のタイミングチャートを示す. 処理は以下のように行われる.

**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.

**CLK3~15:** 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. 鍵スケジューリングは 13 サイクルを要し, 最終サイクル(CLK=15)で Kvld=1 となる. 続いて制御回路はアイドリング状態 “IDLE” を返し, BSY=0 となる.

**CLK16:** 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にストアされる. EncDec=0 であるため, 鍵暗号化処理が実行される.

**CLK17~34:** 暗号化処理が開始され, BSY=1 となる. 暗号化処理は 18 サイクルを要し, 最終サイクル (CLK=34) で Dvld=1 となる. 出力データは CLK=34 でのみ有効である. 続いて制御回路はアイドリング状態 “IDLE” を返し, BSY=0 となる.

**CLK35:** Drdy=1 とすることで, 次のラウンドの処理が開始される. EncDec=1 であるため復号処理が実行される.

**CLK36~54:** 復号処理が開始され, BSY=1 となる. 復号処理は 19 サイクルを要し, 最終サイクル (CLK=54) で Dvld=1 となる. 出力データは CLK=54 でのみ有効である. 続いて制御回路はアイドリング状態 “IDLE” を返し, BSY=0 となる.

# 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 Cryptology (*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. López, 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) K. Itoh, T. Izu, and M. Takenaka, “A practical countermeasure against Address-Bit Differential Power Analysis,” in Cryptographic Hardware and Embedded Systems (*CHES ’03*), LNCS 2779, pp. 382–396, Springer, 2003.
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
27) Sony Corporation, “The 128-bit Block Cipher CLEFIA Algorithm Specification,” Jun. 2007, http://www.sony.co.jp/Products/clefia/technical/data/clefia-spec-1.0.pdf.
28) Sony Corporation, “The 128-bit Block Cipher CLEFIA Security and Performance Evaluations,” Jun. 2007, http://www.sony.co.jp/Products/clefia/technical/data/clefia-eval-1.0.pdf.
29) T. Sugawara, N. Homma, T. Aoki, and A. Satoh, "High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA," Proceedings of 2008 International Symposium on Circuits and Systems (ISCAS2008), pp. 2925--2928, May 2008

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