Specifications

128 ビットブロック暗号 CLEFIA 参照ハードウェア設計記述仕様書

Version 1.0.0 (2010年1月29日)

ソニー株式会社

変更履歴

バージョン	日付	説明
1.0.0	2010年1月29日	初版作成

1. 概要

本仕様書では，CLEFIA 参照ハードウェア設計記述の仕様について述べる．参照ハードウェア設計記述は，MODE, ENCDEC の指定により 128 ビット鍵，192 ビット鍵，256 ビット鍵のCLEFIA の暗復号を行なうことができる．なお，ハードウェア記述言語は Verilog-HDL を用いている．

2. 入出力信号

トップモジュール名: CLEFIA

ポート名	I/O	ビット幅	極性	説明
CLK	I		↑	システムクロック
SRST	I		H	同期リセット
MODE	I	[1:0]	-	00: 128 ビット鍵 CLEFIA, 01: 192 ビット鍵 CLEFIA 10: 256 ビット鍵 CLEFIA
ENCDEC	I		-	0: 暗号化, 1: 復号
KEYSET	I		H	鍵設定信号
DATASET	I		H	平文・暗号文設定信号
KEY	I	[255:0]	-	鍵入力
DIN	I	[127:0]	-	平文・暗号文入力
BSY	O		H	ビジー信号
DVLD	O		H	暗号文・平文出力完了信号
DOUT	O	[127:0]	-	暗号文・平文出力

なお，128 ビット鍵，192 ビット鍵の場合には鍵入力 KEY は LSB 詰めで入力する．つまり，128 ビット鍵 CLEFIA の場合には KEY[127:0] に，192 ビット鍵 CLEFIA の場合には KEY[191:0] に鍵を入力する．

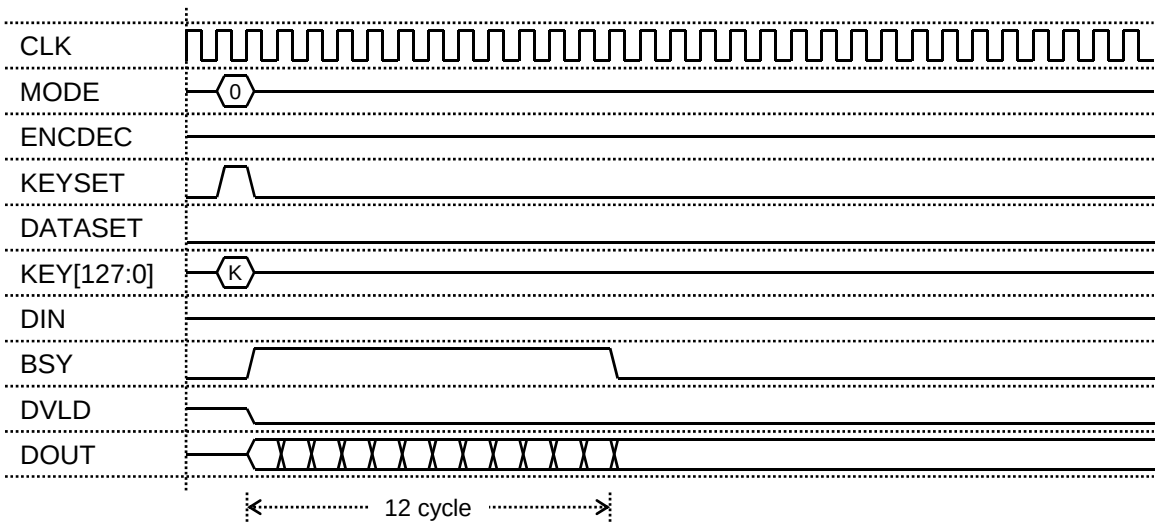
3. タイミングチャート

128 ビット鍵, 192 ビット鍵, 256 ビット鍵 CLEFIA の鍵設定, 暗号化, 復号の各動作について, タイミングチャートを用いて説明を行なう. なお, 最初の鍵設定を行なう前に SRST を 1 クロック以上アサートし制御レジスタの初期化を行なう必要がある.

3.1. 128 ビット鍵 CLEFIA

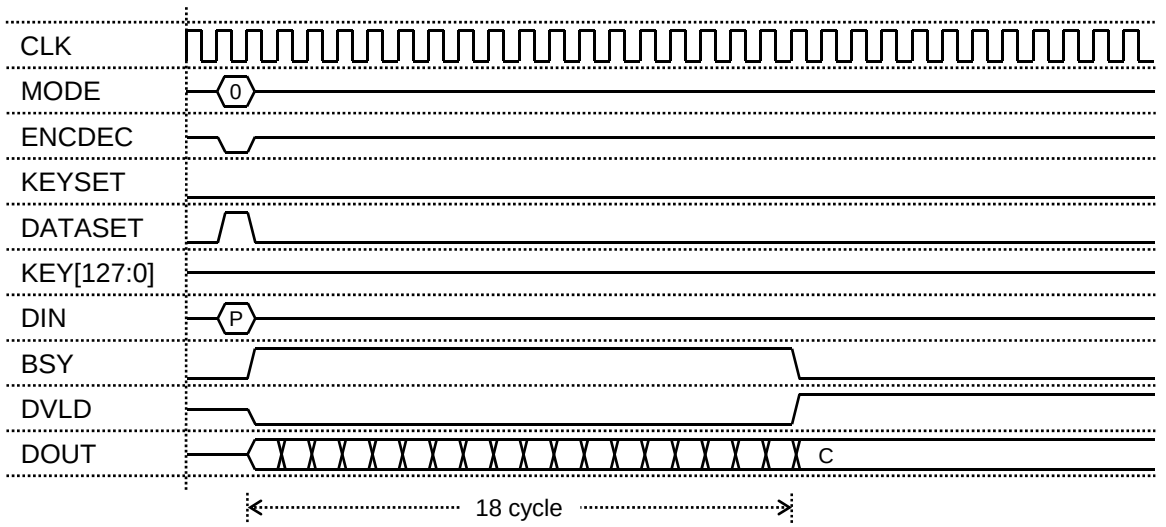
3.1.1. 鍵設定

1. BSY = 0 の状態で MODE に 0 を, KEY[127:0] に 128 ビットの鍵 K を入力し, KEYSET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1, DVLD = 0 となり, KEYSET = 0 とする.
3. 12 サイクル後に BSY = 0 となり鍵設定が完了する.



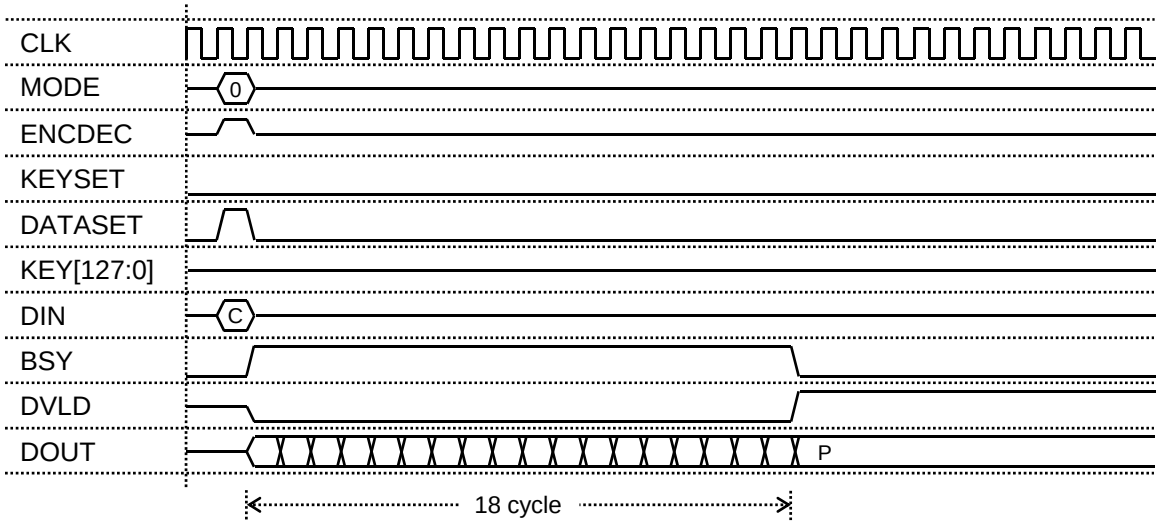
3.1.2. 暗号化

1. 128 ビット鍵 CLEFIA の鍵設定が既に行われた後に, BSY = 0 の状態で MODE に 0 を, ENCDEC に 0 を, DIN に平文 P を入力し, DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1, DVLD = 0 となり, DATASET = 0 とする.
3. 18 サイクル後に BSY = 0, DVLD = 1 となり, DOUT に暗号文 C が出力される.



3.1.3. 復号

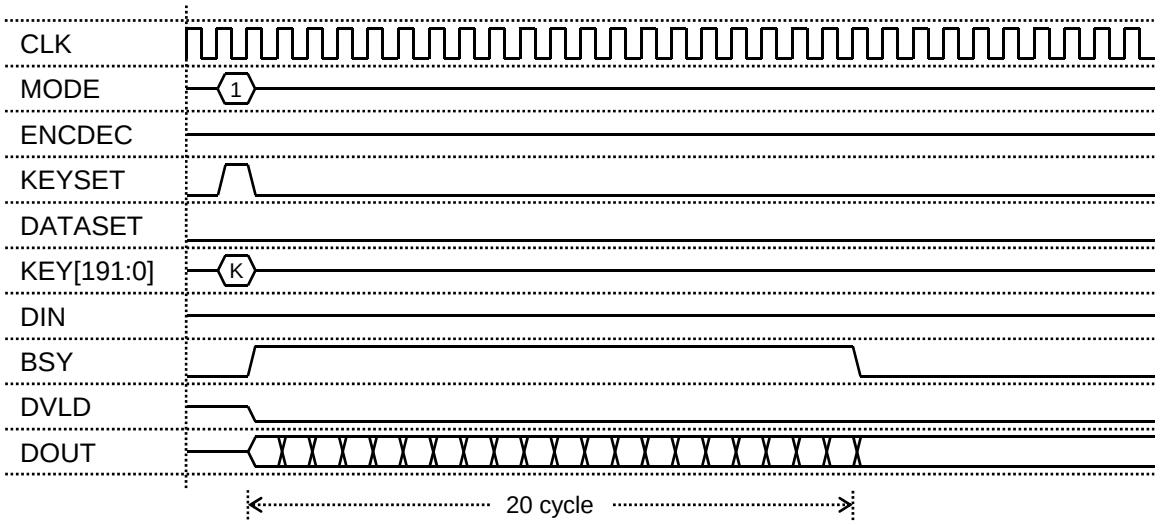
1. 128 ビット鍵 CLEFIA の鍵設定が既に行われた後に，BSY = 0 の状態で MODE に 0 を，ENCDEC に 1 を，DIN に暗号文 C を入力し，DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，DATASET = 0 とする.
3. 18 サイクル後に BSY = 0，DVLD = 1 となり，DOUT に平文 P が出力される.



3.2. 192 ビット鍵

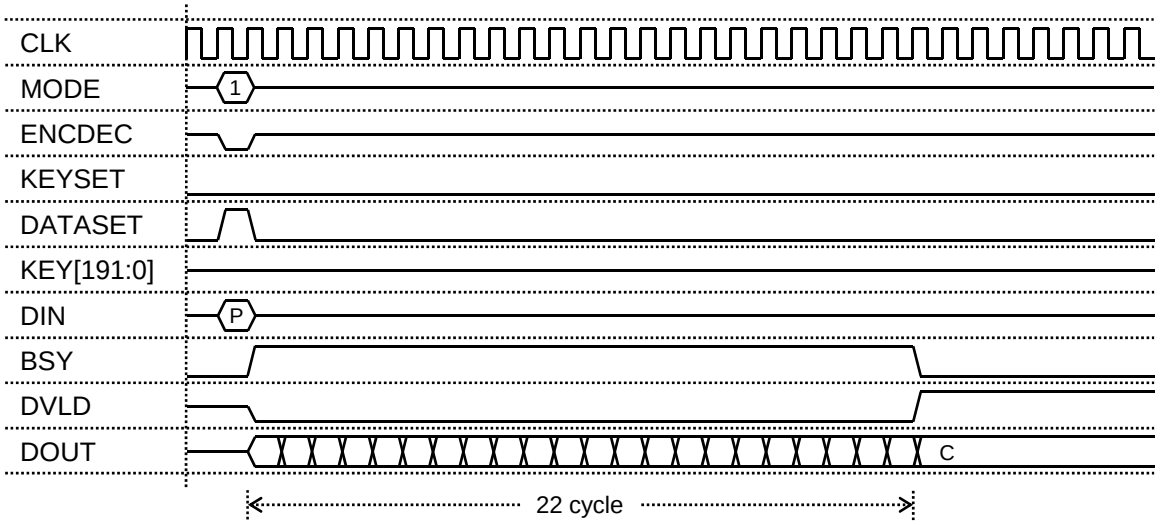
3.2.1. 鍵設定

1. BSY = 0 の状態で MODE に 1 を，KEY[191:0] に 192 ビットの鍵 K を入力し，KEYSET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，KEYSET = 0 とする.
3. 20 サイクル後に BSY = 0 となり鍵設定が完了する.



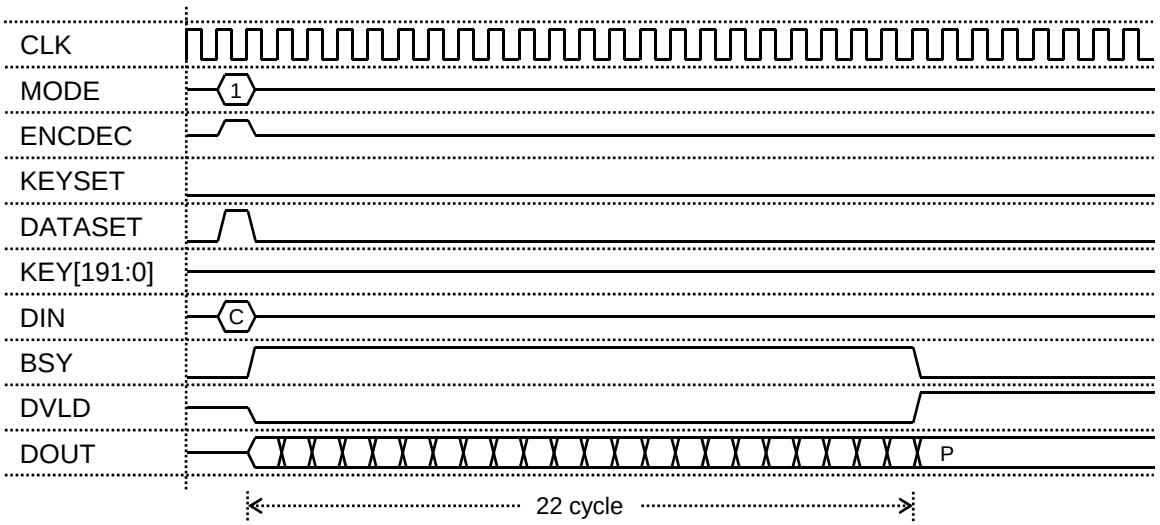
3.2.2. 暗号化

1. 192 ビット鍵 CLEFIA の鍵設定が既に行われた後に，BSY = 0 の状態で MODE に 1 を，ENCDEC に 0 を，DIN に平文 P を入力し，DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，DATASET = 0 とする.
3. 22 サイクル後に BSY = 0，DVLD = 1 となり，DOUT に暗号文 C が出力される.



3.2.3. 復号

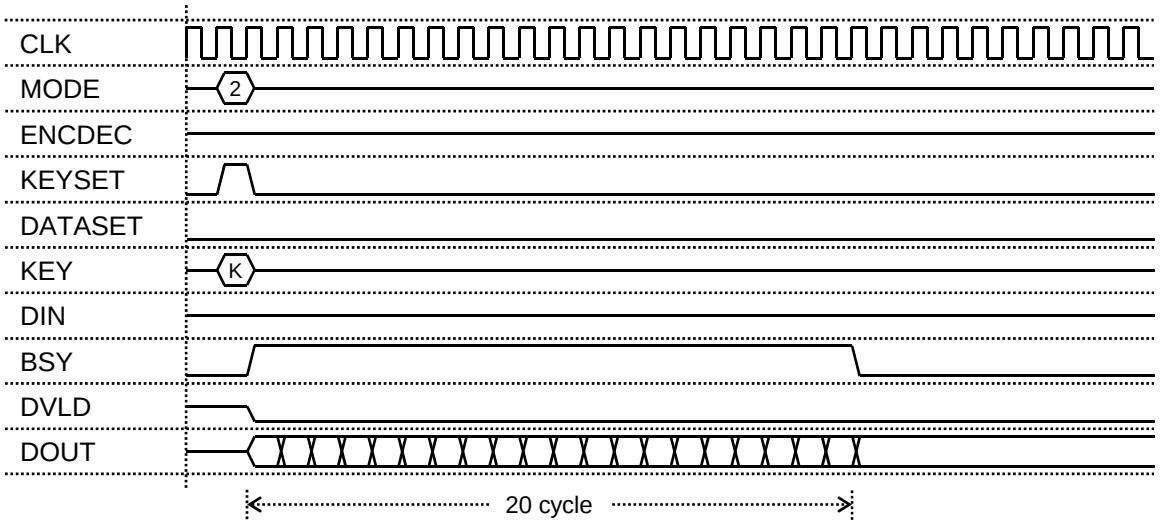
1. 192 ビット鍵 CLEFIA の鍵設定が既に行われた後に，BSY = 0 の状態で MODE に 1 を，ENCDEC に 1 を，DIN に平文 P を入力し，DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，DATASET = 0 とする.
3. 22 サイクル後に BSY = 0，DVLD = 1 となり，DOUT に暗号文 C が出力される.



3.3. 256 ビット鍵

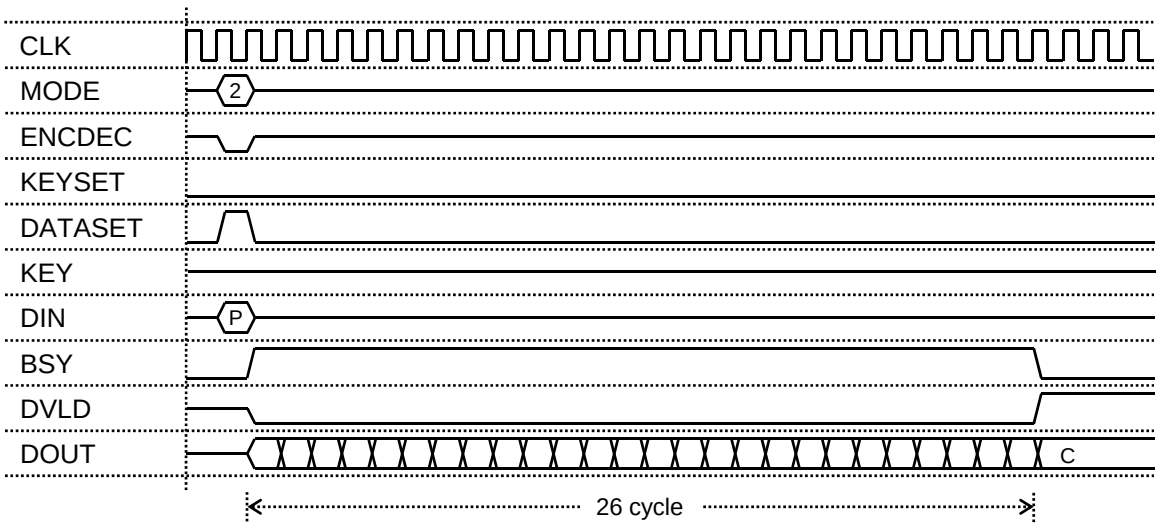
3.3.1. 鍵設定

1. BSY = 0 の状態で MODE に 2 を，KEY に 256 ビットの鍵 K を入力し，KEYSET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，KEYSET = 0 とする.
3. 20 サイクル後に BSY = 0 となり鍵設定が完了する.



3.3.2. 暗号化

1. 256 ビット鍵 CLEFIA の鍵設定が既に行われた後に，BSY = 0 の状態で MODE に 2 を，ENCDEC に 0 を，DIN に平文 P を入力し，DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，DATASET = 0 とする.
3. 26 サイクル後に BSY = 0，DVLD = 1 となり，DOUT に暗号文 C が出力される.



3.3.3. 復号

1. 256 ビット鍵 CLEFIA の鍵設定が既に行われた後に，BSY = 0 の状態で MODE に 2 を，ENCDEC に 1 を，DIN に暗号文 C を入力し，DATASET = 1 とする.
2. 次の CLK の立ち上がりで BSY = 1，DVLD = 0 となり，DATASET = 0 とする.
3. 26 サイクル後に BSY = 0，DVLD = 1 となり，DOUT に暗号文 P が出力される.