Specifications

128-bit blockcipher CLEFIA reference HDL code specifications

Version 1.0.0 (January 29, 2010)

Sony Corporation

Change History

Version	Date	Description
1.0.0	January 29, 2010	Created

1. Overview

This document describes specifications of the reference HDL code of CLEFIA. The reference HDL code supports encryption and decryption of CLEFIA with 128-bit key, 192-bit keys and 256-bit keys by choosing MODE and ENCDEC. The reference HDL code is written in Verilog-HDL.

2. I/O ports

top module name: CLEFIA

port name	I/O	bit width	active	description
CLK	I		↑	system clock
SRST	I		H	synchronous reset
MODE	I	[1:0]	-	00: CLEFIA with 128-bit keys 01: CLEFIA with 192-bit keys 10: CLEFIA with 256-bit keys
ENCDEC	I		-	0: encryption 1: decryption
KEYSET	I		H	key set signal
DATASET	I		H	plaintext/ciphertext set signal
KEY	I	[255:0]	-	key input
DIN	I	[127:0]	-	plaintext/ciphertext input
BSY	O		H	busy signal
DVLD	O		H	data output valid sinal
DOUT	O	[127:0]	-	ciphertext/plaintext output

For CLEFIA with 128-bit keys, 128-bit keys must be input to KEY[127:0]. For CLEFIA with 192-bit keys, 192-bit keys must be input to KEY[191:0].

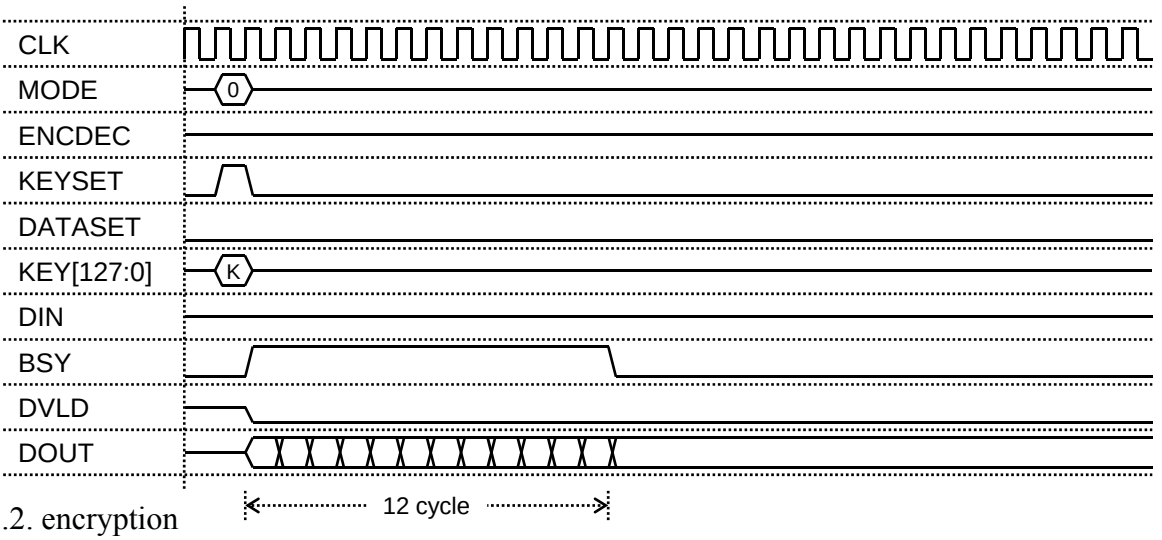
3. Timing Chart

We describe how to operate the reference HDL codes in key setup, encryption and decryption for CLEFIA with 128-bit keys, 192-bit keys and 256-bit keys. It is necessary to initialize control registers by asserting SRST in at least one cycle before first key setup.

3.1. CLEFIA with 128-bit keys

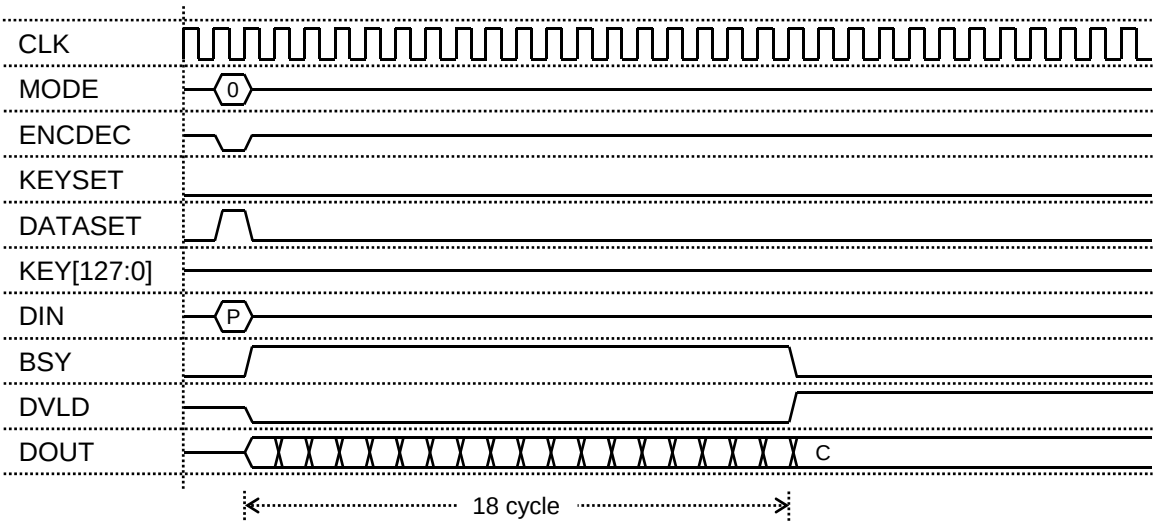
3.1.1. key setup

1. Input 0 and a 128-bit key K to MODE and KEY[127:0], respectively. Assert KEYSET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert KEYSET = 0.
3. After 12 cycles of CLK, BSY is set to 0. Key setup is completed .



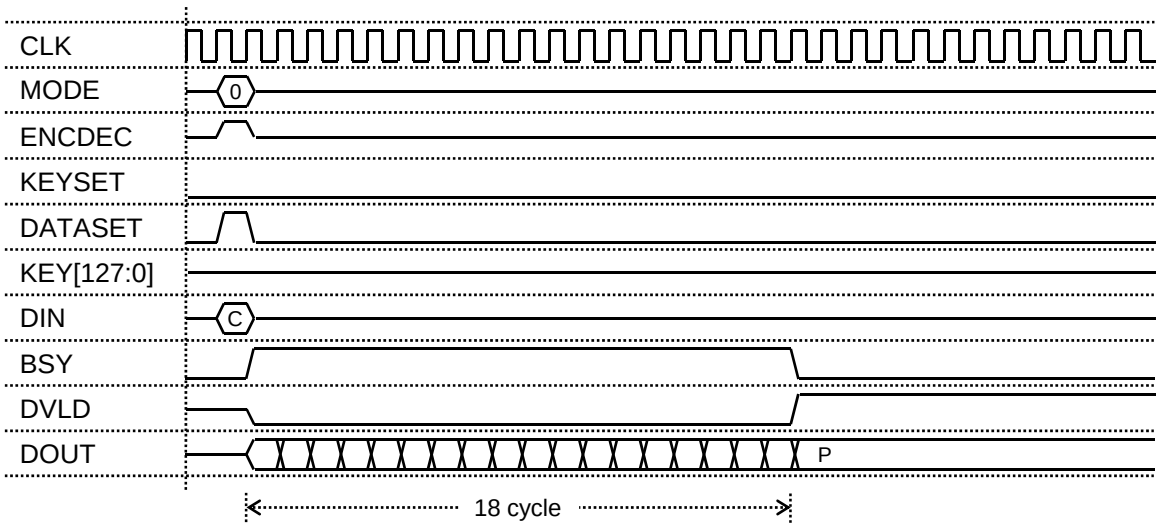
3.1.2. encryption

1. After key setup for CLEFIA with 128-bit keys is completed, input 0, 0 and a plaintext P to MODE, ENCDEC and DIN, respectively. Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 18 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A ciphertext C is output from DOUT.



3.1.3. decryption

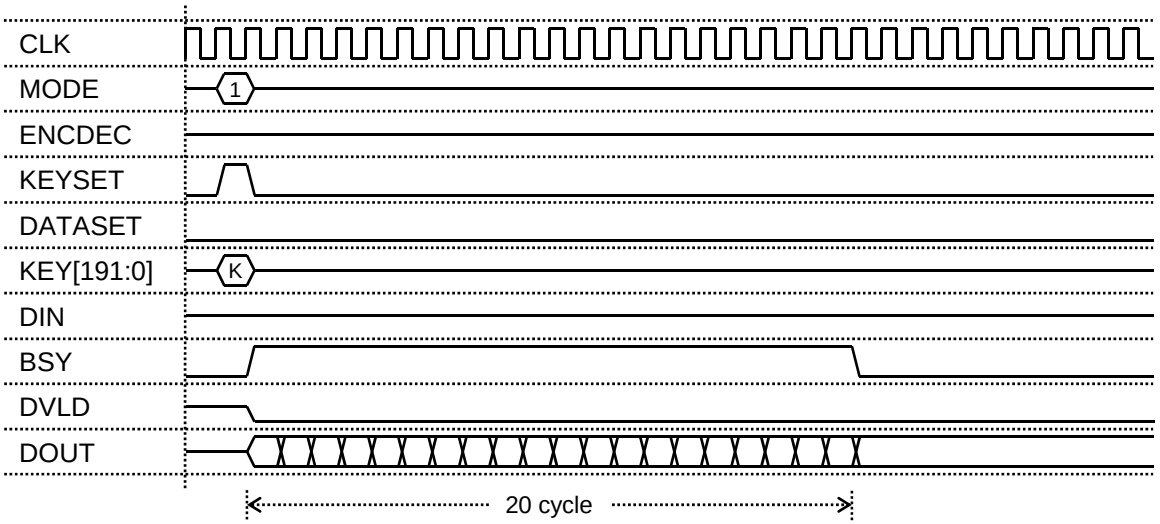
1. After key setup for CLEFIA with 128-bit keys is completed, input 0, 1 and a ciphertext C to MODE, ENCDEC and DIN, respectively. Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 18 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A plaintext P is output from DOUT.



3.2. CLEFIA with 192-bit keys

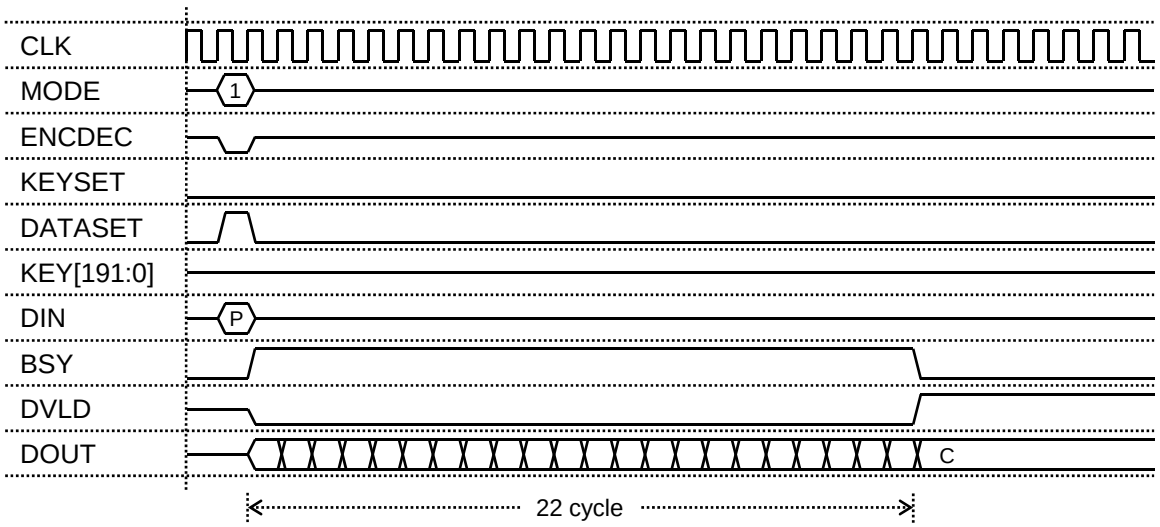
3.2.1. key setup

1. Input 1 and a 192-bit key K to MODE and KEY[191:0], respectively. Assert KEYSET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert KEYSET = 0.
3. After 20 cycles of CLK, BSY is set to 0. Key setup is completed .



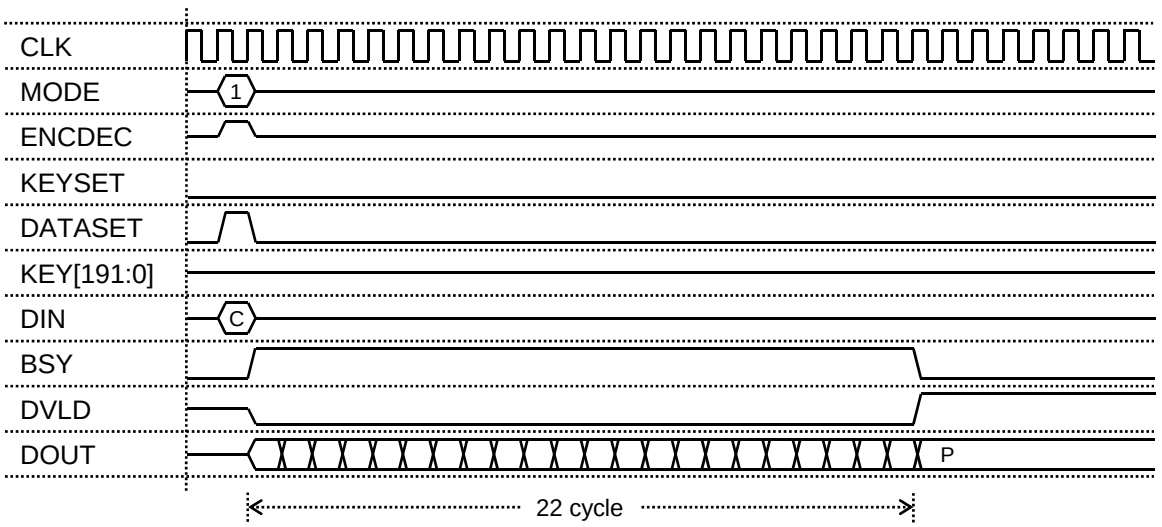
3.2.2. encryption

1. After key setup for CLEFIA with 192-bit keys is completed, input 1, 0 and a plaintext P to MODE, ENCDEC and DIN, respectively. Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 22 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A ciphertext C is output from DOUT.



3.2.3. decryption

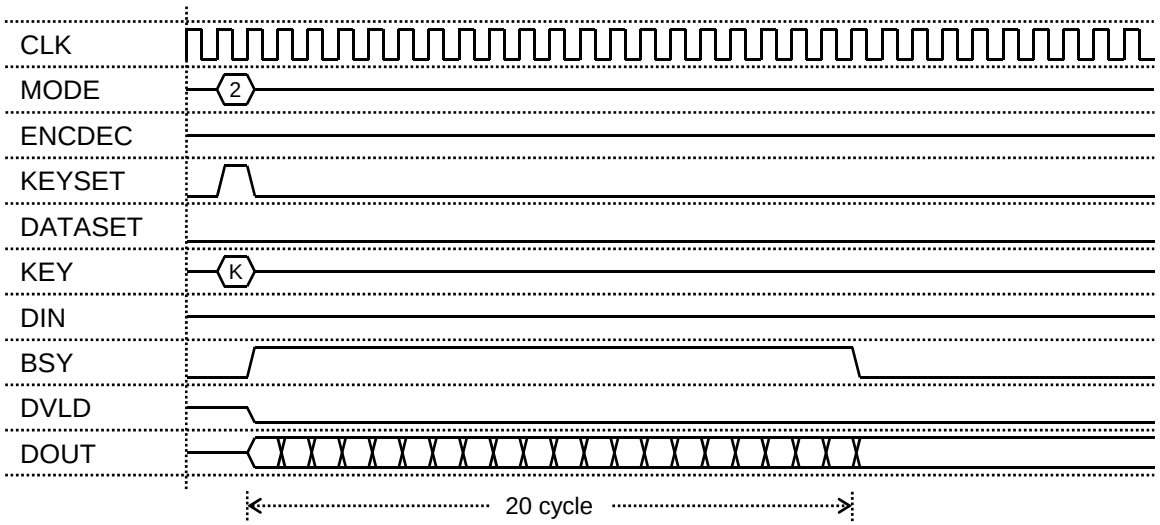
1. After key setup for CLEFIA with 192-bit keys is completed, input 1, 1 and a ciphertext C to MODE, ENCDEC and DIN, respectively. Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 22 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A plaintext P is output from DOUT.



3.3. CLEFIA with 256-bit keys

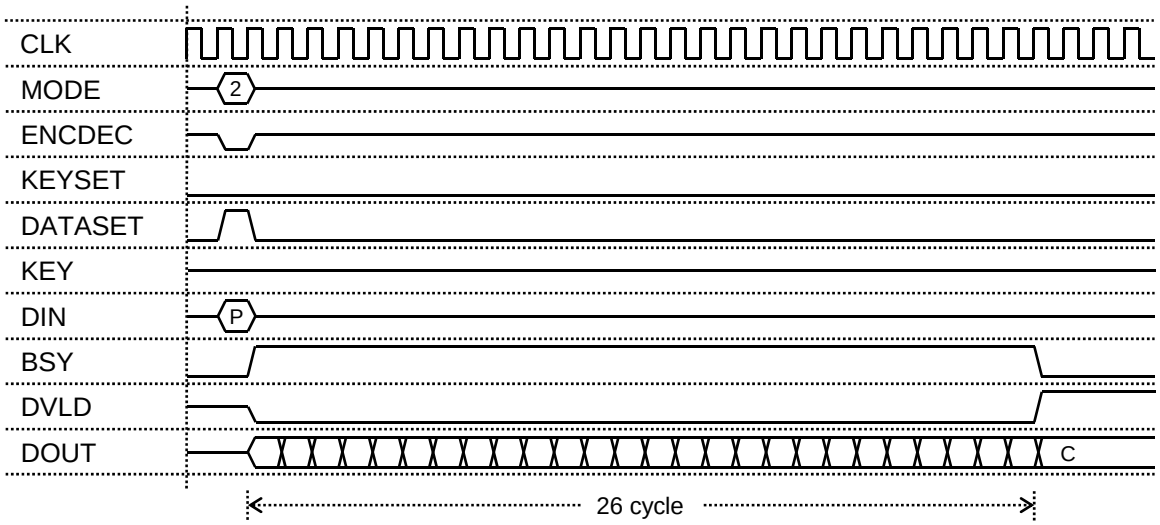
3.3.1. key setup

1. Input 2 and a 256-bit key K to MODE and KEY, respectively. Assert KEYSET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert KEYSET = 0.
3. After 20 cycles of CLK, BSY is set to 0. Key setup is completed .



3.3.2. encryption

1. After key setup for CLEFIA with 256-bit keys is completed, input 2, 0 and a plaintext P to MODE, ENCDEC and DIN, respectively Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 26 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A ciphertext C is output from DOUT.



3.3.3. decryption

1. After key setup for CLEFIA with 256-bit keys is completed, input 2, 1 and a ciphertext C to MODE, ENCDEC and DIN, respectively. Assert DATASET = 1 when BSY = 0.
2. BSY and DVLD are set to 1 and 0, respectively, at the next rising edge of CLK. Deassert DATASET = 0.
3. After 26 cycles of CLK, BSY and DVLD is set to 0 and 1, respectively. A plaintext P is output from DOUT.