Stream Cipher
Enocoro-128v2

Specification for The Reference Hardware Description

Hitachi, Ltd.

2 February 2010

Contents

Copyright ©2009-2010 Hitachi, Ltd. All rights reserved.

1. Introduction

This documentation gives the specification for the reference hardware description of *Enocoro*-128v2. It gives the pseudorandom number generation function which is the core function of the stream cipher.

2. Module specification

2.1 Module overview

This hardware description gives the following module (Table 1).

Table 1. Module list

#	Name	Faculty
1	enocoro_128()	pseudorandom number generation

(1) When Key & IV input enable signal (input_set) is asserted, the module retrieves Key input data (Key_in) and Initial value input data (iv_in) and starts the initialization process.

(2) When finishing the initialization process, the module is ready for outputting pseudorandom number data and asserts pseudorandom number output ready signal (output_ready).

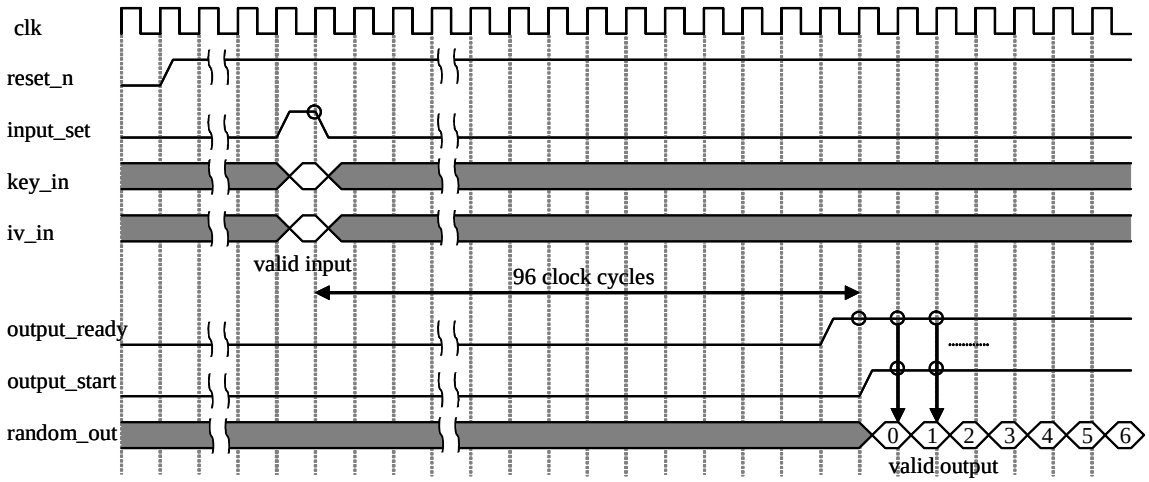
(3) When both pseudorandom number output ready signal (output_ready) and pseudorandom number output startsignal (output_start) are asserted, the module outputs valid pseudorandom number output data (random_out) per clock cycle.

2.2 Pin list

#	Pin name	I/O	description
1	reset_n	I	Reset signal
2	Clk	I	Clock
3	key_in[127:0]	I	Key input data
4	iv_in[127:0]	I	Initial value input data
5	input_set	I	Key & IV input enable signal
6	output_start	I	pseudorandom number output start signal
7	output_ready	O	pseudorandom number output ready signal
8	random_out[7:0]	O	pseudorandom number output data

Copyright ©2009-2010 Hitachi, Ltd. All rights reserved.

2.3 Timing chart



3. File list

Table 2 shows the file list of the hardware description.

Table 2. File list

#	File type	File name	Contents
1	Verilog	eocoro.v	Main module

Copyright ©2009-2010 Hitachi, Ltd. All rights reserved.