ストリーム暗号　*Enocoro*-128v2

参照ハードウェア設計記述仕様書

株式会社 日立製作所

2010 年 2 月 2 日

目次

１．はじめに

本ドキュメントは、ストリーム暗号 *Enocoro*-128v2 の参照ハードウェア設計記述の仕様書である。本モジュールは、ストリーム暗号のコアである疑似乱数生成機能を提供する。

２．モジュール仕様

２．１ 機能概要

本参照ハードウェア設計記述で提供するモジュールを表 1に示す。

表 1. 提供モジュール

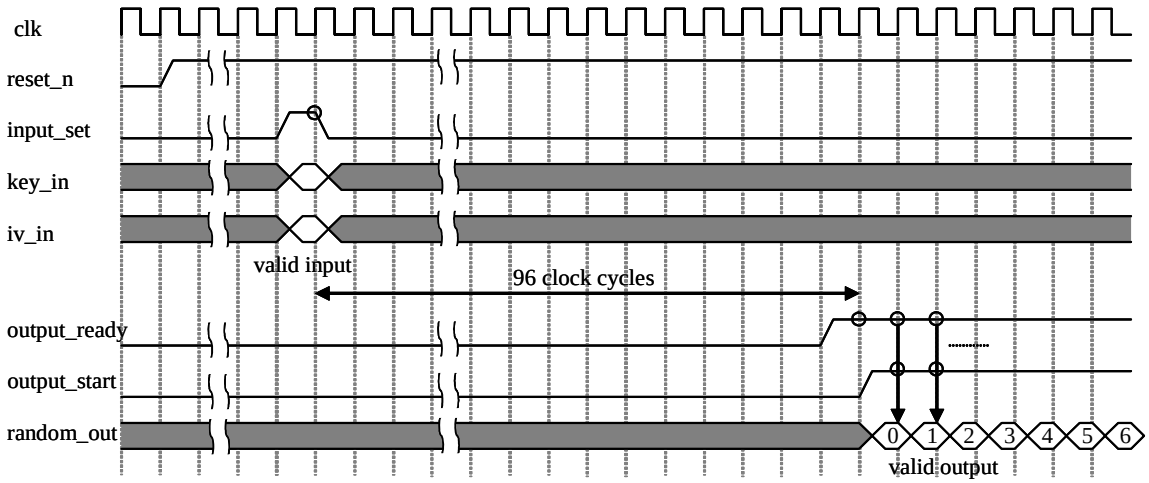
#	名称	機能概要
1	enocoro_128()	乱数列の出力

(1) 入力データイネーブル信号 input_set のアサート時に、鍵入力データ key_in、及び、初期値入力データ iv_in を取り込み、初期化動作を開始する。
(2) 上記初期化動作が終了し、疑似乱数出力準備が整った時点で、出力データレディ信号 output_ready をアサートする。
(3) 出力データイネーブル信号 output_ready アサート、且つ、疑似乱数出力開始指示信号 output_start アサート時に、クロック毎に有効な疑似乱数出力データ random_out を出力する。

２．２ ピンリスト

#	pin name	I/O	description
1	reset_n	I	初期化
2	clk	I	クロック
3	key_in[127:0]	I	鍵入力データ
4	iv_in[127:0]	I	初期値入力データ
5	input_set	I	入力データイネーブル信号
6	output_start	I	疑似乱数出力開始指示信号
7	output_ready	O	出力データレディ信号
8	random_out[7:0]	O	疑似乱数出力データ

２．３ タイミングチャート



３．ファイル一覧

本参照ハードウェア設計記述のファイルを表 2に示す。

表 2. ファイル一覧

#	ファイルタイプ	ファイル名	内容
1	Verilog	eocoro.v	処理モジュール本体