AES256IP Reference Design

Rev1.00 10-Sep-2021

1 Introduction

This document describes detailed of AESIP256IP reference design. In this reference design, AES256IP are applied to encrypt data to NVMe SSD and decrypt data from NVMe SSD. This document will show detail of hardware design and detail of AES256IP in both encryption section and decryption section

2 Hardware Overview

AES256IP reference design is based on NVMe-IP reference design. Figure 2-1 show NVMe-IP reference design block diagram. The operation of NVMe-IP start by Test PC send write or read command parameter to TestGen module. Then TestGen module start write or read pattern data from or to NVMe SSD via FIFO 128-bit. NVMe-IP manage pattern data between FIFO 128-bit and NVMe SSD.

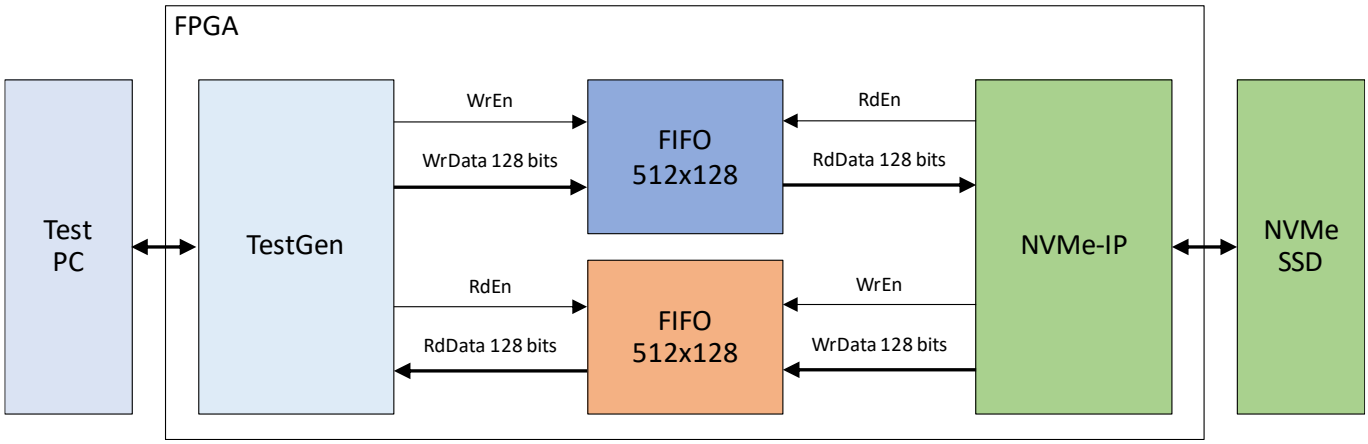

Figure 2-1 NVMe-IP reference design block diagram

For more detail of NVMe-IP reference design, please see "**NVMe-IP reference design manual**" document

(download link is https://dgway.com/products/IP/NVMe-IP/dg_nvmeip_refdesign_intel_en.pdf).

3 AES256IP reference design

AES256IP reference design has concept to encrypt and decrypt data from or to NVMe SSD. So AES256IP is applied to NVMe-IP reference design. Both FIFO 128-bit are replaced by AES256IP. One FIFO is replaced by AES256 encryption module (TopAESENC), the other FIFO is replaced by AES256 decryption module (TopAESDEC). Figure 3-1 shows AES256IP was applied to NVMe-IP reference design.

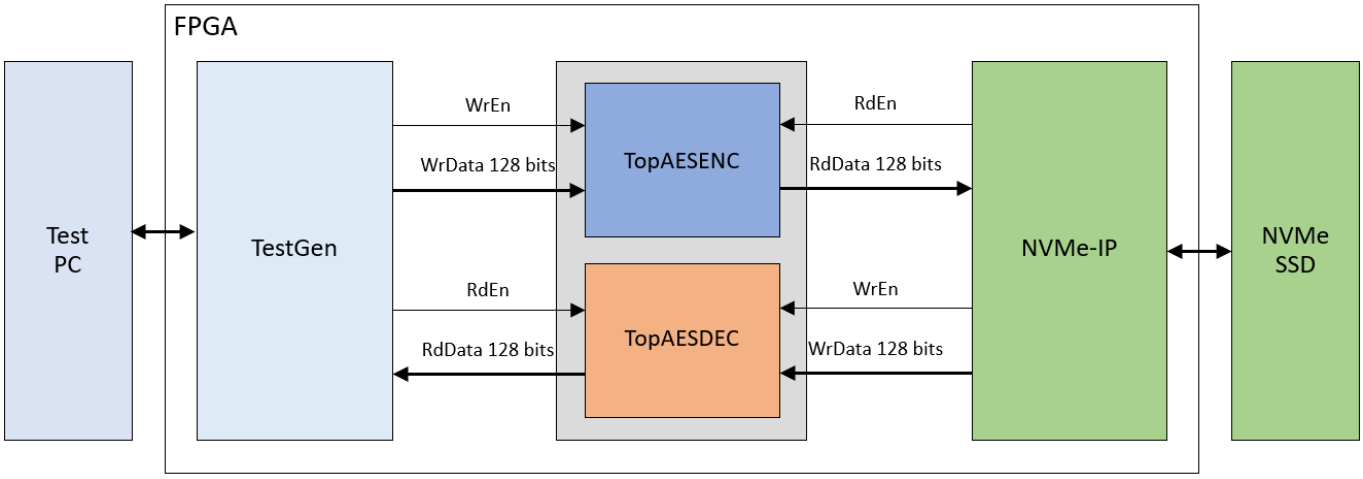

Figure 3-1 AES256IP reference design block diagram

3.1 TopAESENC

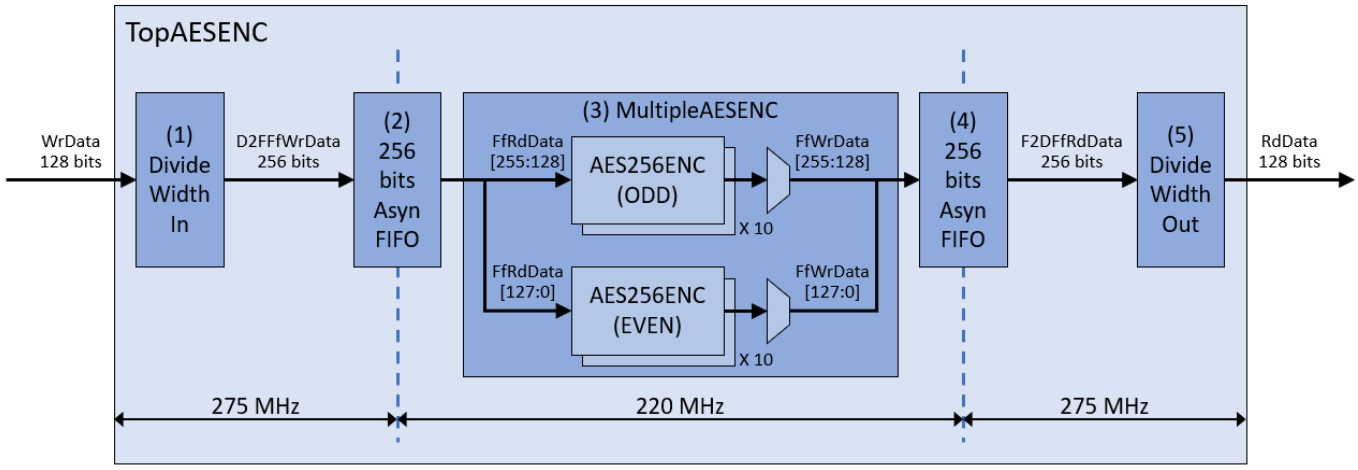

Figure 3-2 TopAESENC block diagram

Figure 3-2 show block diagram of TopAESENC that has 5 blocks. The details of each block are shown below.

1. DivideWidthIn

According to best NVMe-IP performance run at 128-bit at clock 275 MHz, and maximum clock frequency of AES256ENC is 250 MHz. So DivideWidthIn is designed to combine 2 cycles of 128-bit input data to be 256-bit data in one cycle, then AES256ENC can run at lower frequency and keep best NVMe-IP performance.

2. 256-bit AsyncFIFO input

According to use the same clock PLL that generate 275 MHz, 220 MHz clock frequency is generated to use in MultipleAESENC module. So, 256-bit AsyncFIFO is designed to transit clock boundaries from 275 MHz to 220 MHz.

3. MultipleAESENC

According to AES256ENC can encrypt rate at 15 clocks / 128-bit data. So MulitpleAESENC is designed to use 20 AES256ENC modules working parallelly to keep best NVMe-IP performance. Because bandwidth of 256-bit x 220MHz x 10/15 is more than 128-bit x 275MHz.

The data input from 256-bit AsyncFIFO is separated to FfRdData[255:128] for 10 modules of AES256ENC(ODD), and FfRdData[127:0] for 10 modules of AES256ENC(EVEN). Then the output data of all AES256ENC will be selected by multiplexer and write to 256-bit AsyncFIFO output.

4. 256-bit AsynFIFO output

This asynchronous FIFO use for transition clock boundaries from 220 MHz to 275 MHz.

5. DivideWidthOut

DivideWidthOut is designed to split 256-bit data in one cycle to be 2 cycles of 128-bit data, when NVMe-IP read data from asynchronous FIFO.

3.2 TopAESDEC

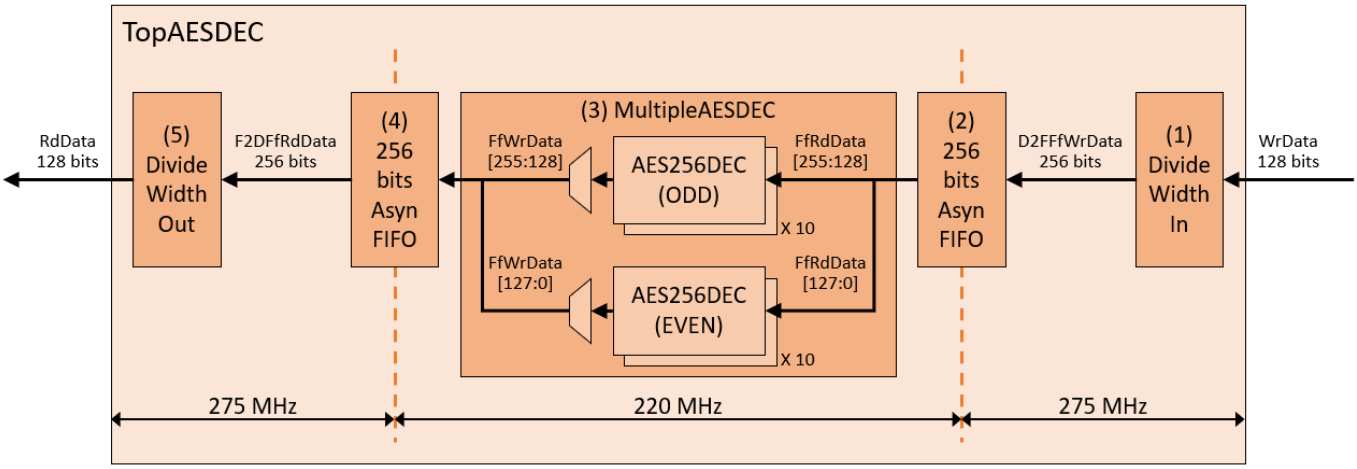

Figure 3-3 TopAESDEC block diagram

Figure 3-3 show block diagram of TopAESDEC that has 5 blocks. The details of each block are shown below.

The detailed design concept of TopAESDEC is as same as TopAESENC in the opposite way.

4 Revision History

Revision	Date	Description
1.00	10-Sep-2021	Initial version release