Low Gate Count AES Core

Features

- **Implement the standard AES encryption/decryption algorithm published in FIPS PUB 197**
- **Support keys of 128, 192 and 256 bits**
- **Integrated key expand unit and programmable encryption/decryption function**
- **Compact design, uses 293 CLB slices and 1 block ram in Vietex IV implementation, among the smallest on the market**
- **Maximum clock speed reaches 318 MHz in Virtex IV implementation, data throughput reaches 904 Mbps**
- **Fully synchronous one clock design**
- **Latency equals 4 * (rounds + 1) + 1**
- **Work with all the modes, i.e. CBC, CFB, OFB, CTR mode, wrapping logic is free**

Pin Out

Figure 1 is the schematic symbol of the AES core. Following is the pin description.

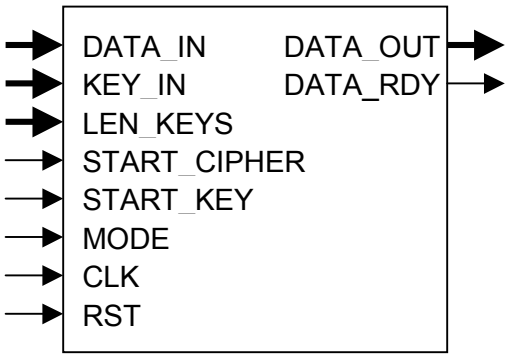

Figure 1. The AES schematic symbol.

RST
One bit input, the asynchronous reset. When RST is set high, all the internal flip-flops are asynchronously initialized. The core will stay in this state until RST is set low.

CLK
One bit input, the global clock. All sequential logic acts on the rising edge of CLK.

MODE
One bit input, the signal to select the function of the core. When mode is 0, the core performs encryption. When mode is 1, the core performs decryption.

START_KEY
One bit input, the signal to start the key expansion unit. At the rising edge of the cock, if START_KEY is high, the key expand unit will start to read in the key, expand the key, and write the expanded key to the internal RAM. Since the encryption and the decryption process use the same key schedule, there is no need to expand the key for both process. Also, if the key does not change for multiple data blocks, there is no need for key expansion for every data block.

START_CIPHER
One bit input, the signal to start the cipher/decipher unit. At the rising edge of the clock, if START_CIPHER is high, the cipher/decipher unit will start to read in the data and encrypt/decrypt the data. For encryption, START_CIPHER must be at least three clocks behind START_KEY when the key is FIRST expanded. For decryption, START_CIPHER must be at least 4*(rounds+1)+1 clocks behind START_KEY when the key is FIRST expanded.

LEN_KEYS
Two bit input, the signal to indicate the length of the keys. If LEN_KEYS is 00, the length of the keys is 128 bits. If LEN_KEYS is 01, the length of the keys is 192 bits. If LEN_KEYS is 10, the length of the keys is 256 bits.

KEY_IN
Thirty-two bit input, the input key.

DATA_IN
Thirty-two bit input, the input data.

DATA_OUT
Thirty-two bit output, the encrypted/decrypted data output.

DATA_RDY
One bit output, the signal to indicate that the output data is ready.

Timing Diagrams

Integration of the core is very easy. The following timing diagrams depict some of the synchronization issues.

Figure 2 shows the timing diagram at the starting point of the key expansion, where K0 is the first 32 bits of the key.

Figure 3 shows the timing diagram at the starting point of the encryption/decryption process, where D0 is the first 32 bits of the data.

Figure 4 shows the timing diagram at the starting point of the output, where O0 is the first 32 bits of the output data.

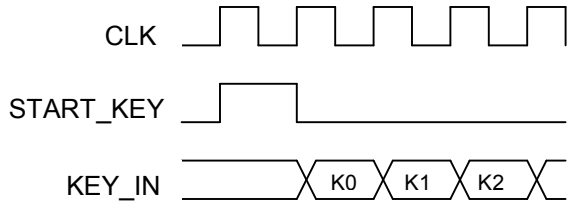

Figure 2. The timing diagram at the starting point of key expansion.

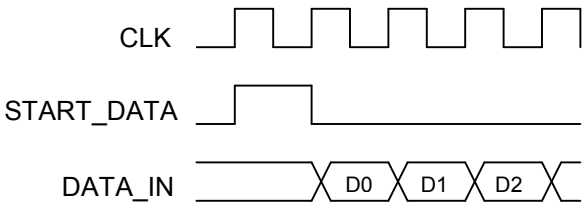

Figure 3. The timing diagram at the starting point of encryption/decryption.

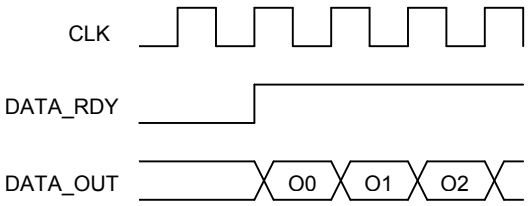

Figure 4. The timing diagram at the starting point of the output

Deliverables

Deliverables include the AES core and the test bench. For Xilinx FPGA implementation, both source code and netlist are available. For ASIC implementation, only source code will be delivered. Source code can be in VHDL or Verilog.

Ordering Information

We have flexible licensing structures. Please use the following information to contact us:

Highland Communications Technologies
928 Concession Road, Fort Erie
Ontario, Canada L2A 6B8

Tel: 1-905-658-0989
Fax: 1-905-248-5188
Email: sales@highlandcomm.com

Web site:
http://www.highlandcomm.com/