Simple Camellia Crypto Core

By:: Ahmad Rifqi H
mr_rifqi@yahoo.com

www.ic.vlsi.itb.ac.id/~rifqi
October 5, 2004

1.Introduction

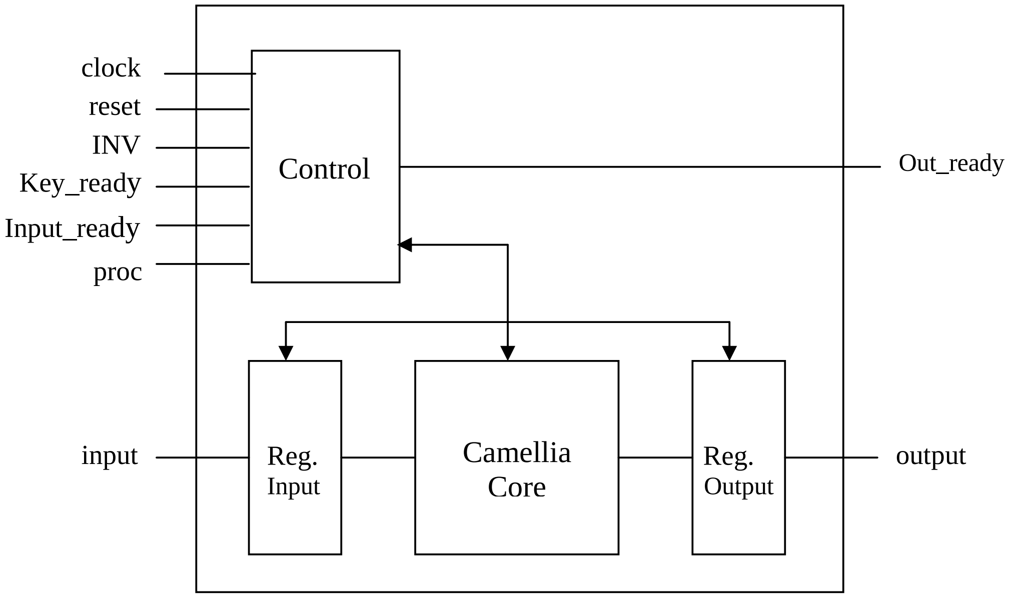
Simple Camellia-128 IP Core. The number “128” noted that this implementation use 128 bit key length. I have implemented this design in Xilinx FPGA board with device target Xilinx XC2V2000 ff896. In-circuit verification has been done using ChipScope 6.2i

This document will describe the interface to the IP core.

2.Architecture

The Camellia-128 core both of encryption or decryption with the same core.
Below figure illustrates the overall architecture of the Camellia-128 core.

Figure 1: Camellia-128 Core Architecture Overview



3. IOs

Name	**Width (bit)**	**Direction**	**Description**
clock	1	**I**	clock signal
reset	1	**I**	reset pin (*active high*, synchronous)
INV	1	**I**	mode select 0 = encryption, 1 = decryption
Key_ready	1	**I**	load key pin (*active high*)
Input_ready	1	**I**	load data pin (*active high*)
Out_ready	1	**O**	data output valid (*active high*)
Input	128	**I**	input text block
output	128	**O**	output text block

4. Operation

This cipher core can perform a complete encrypt or decrypt sequence in 10 clock cycles. 1 cycle to load the key, 2 cycle to process the key (setup key), 1 cycle to load the data and 6 cycle to process the data (encryption / decryption).

The INV pin must be set or reset to select the mode operation, ‘0’ = emcryption, ‘1’= decryption.

When the core completes the encryption/decryption sequence it will assert the ‘out_ready’ signal for one clock cycle to indicate the completion. The user might chose to ignore the ‘done’ output and time the completion of the encryption sequence externally.

Figure 2: Camellia-128 Core Encryption process

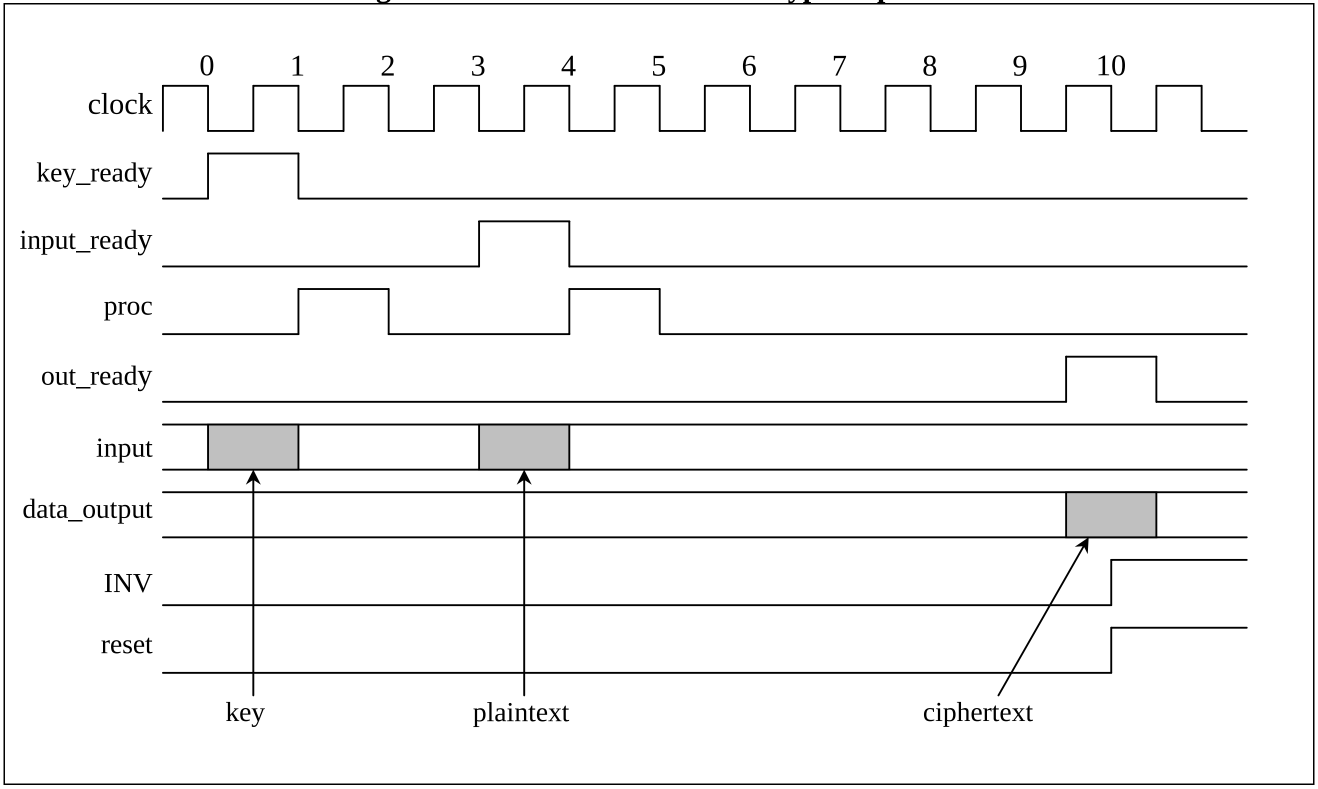
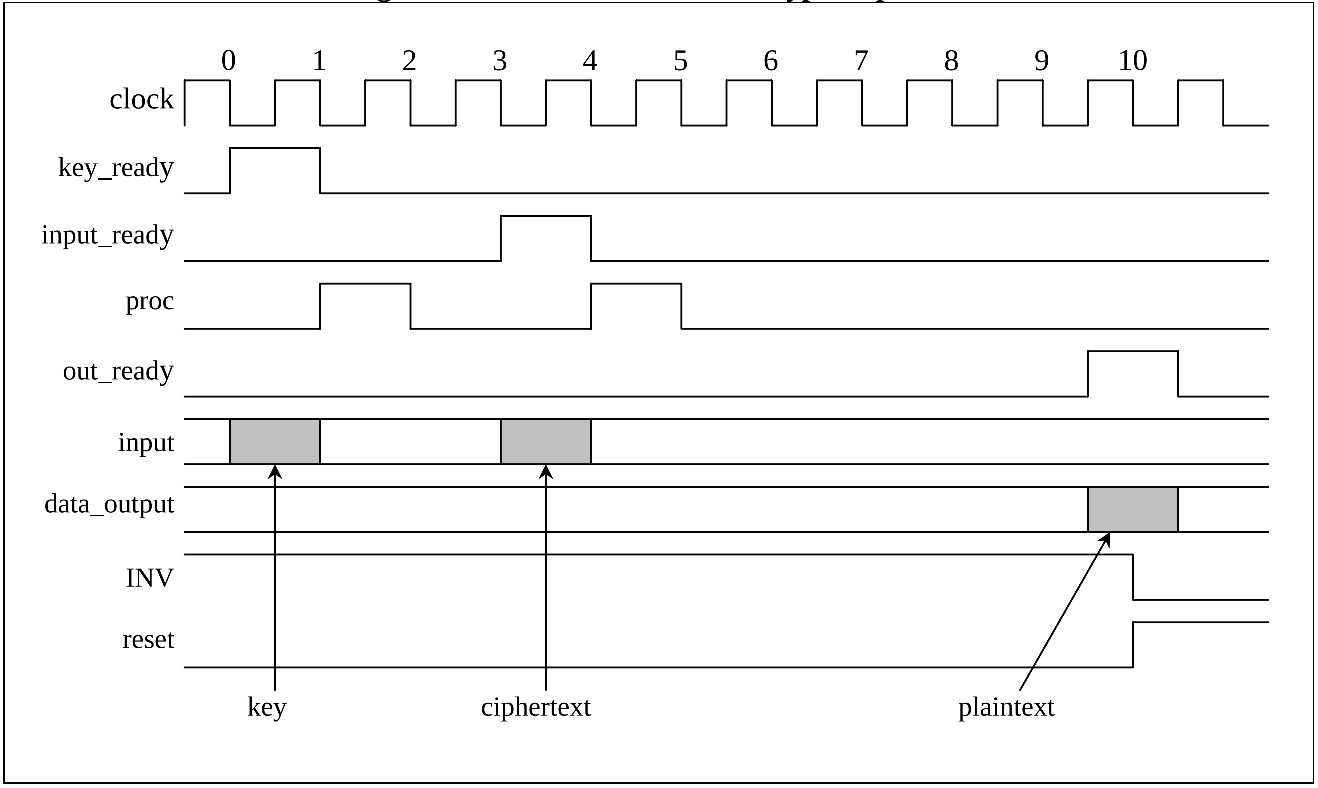


Figure 3: Camellia-128 Core Decryption process


0
1
2
3
4
5
6
7
8
9
10
clock
key_ready
input_ready
proc
out_ready
input
data_output
INV
reset
key
ciphertext
plaintext