ADVANCED ENCRYPTION STANDARD

Name	Description	
CC-AES-APB-AHB	Advanced Encryption Standard Core with APB Interface	
Category	**Type**	**Status**
Cryptographic Cores	AES	Silicon and FPGA Proven
Deliverables		
♦ Unencrypted RTL code ♦ User manual ♦ Testbench	♦ C header file ♦ Support	
Features		
♦ AMBA APB3 bus ♦ Encryption and/or decryption ♦ ECB mode ♦ 128 bit data block ♦ Programmable 128, 192, 256 bit key length	♦ Fully synthesizable synchronous design with positive edge clocking ♦ DFT ready ♦ Technology independent IP Core ♦ Flexible licensing scheme	

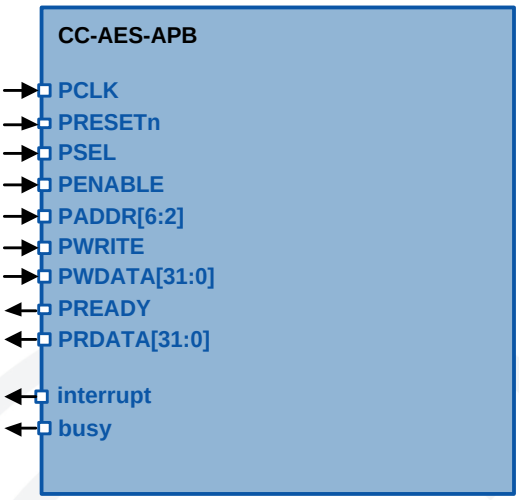

Figure 1. Symbol.

Table 1. Throughput (including interface).

Key length	Throughput
128-bit	4.13 bits/cycle
192-bit	3.88 bits/cycle
256-bit	3.66 bits/cycle

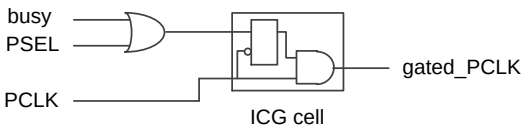

Figure 2. Integration example. Using clock_request pin for low power mode

ChipCraft Sp. z o.o.
Bukowinska 22 lok. 9B
02-703 Warsaw, POLAND

www.chipcraft-ic.com

Table 2. Pin description.

Pin name	Direction	Active	Description
PCLK	I	rising	Synchronous clock
PRESETn	I	low	Asynchronous reset
PSEL	I	high	APB peripheral select
PENABLE	I	high	APB bus enable
PADDR[6:2]	I	data	APB bus address
PWRITE	I	high	APB bus write
PWDATA[31:0]	I	data	APB bus write data
PREADY	O	high	APB bus ready
PRDATA[31:0]	O	data	APB bus read data
interrupt	O	high	AES interrupt
busy	O	high	AES busy

Table 3. Generic Parameters.

Generic name	Type	Range	Description
DECRYPTION_PATH	integer	0, 1	Configure AES core decryption support

ChipCraft Sp. z o.o.
Bukowinska 22 lok. 9B
02-703 Warsaw, POLAND

www.chipcraft-ic.com