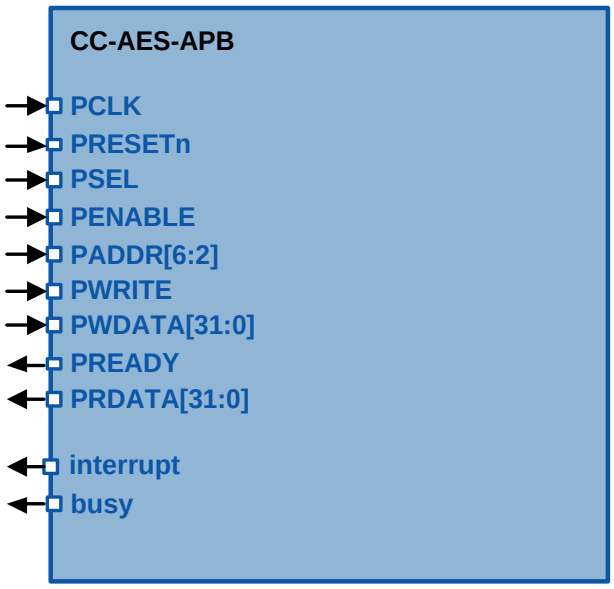
CC-AES-APB Advanced Encryption Standard Core

Symbol



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

Benefits

- Supplied as human-readable Verilog RTL source code
- Technology independent IP Core
- Suitable for FPGA and ASIC
- Easy SoC integration
- Full implementation and maintenance support with individual approach
- Flexible licensing scheme

Throughput (including interface)

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

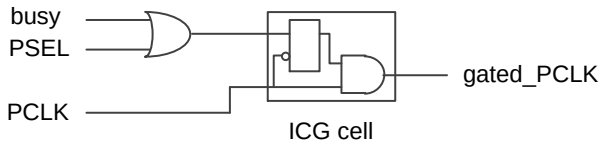
office@chipcraft-ic.com
www.chipcraft-ic.com

Generic Parameters

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

Integration example

- Using clock_request pin for low power mode:



Pin-out Description

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