SILVACO

AHB AES with DMA

The Advanced Encryption Standard (AES) IP Core is a complete hardware implementation encryption/decryption algorithm described in the U.S. Government Federal Information Processing Standards Publication 197 (FIPS 197). The AES IP Core implements the Rijndael algorithm which is a symmetric block cipher that can process 128-bit data blocks using 128, 192, or 256-bit cipher keys. The United States Government designed the Advanced Encryption Standard (AES) in 2000 to replace the older Data Encryption Standard (DES). AES is a symmetric block cipher which means that the same key is used for both encryption and decryption of the data block.

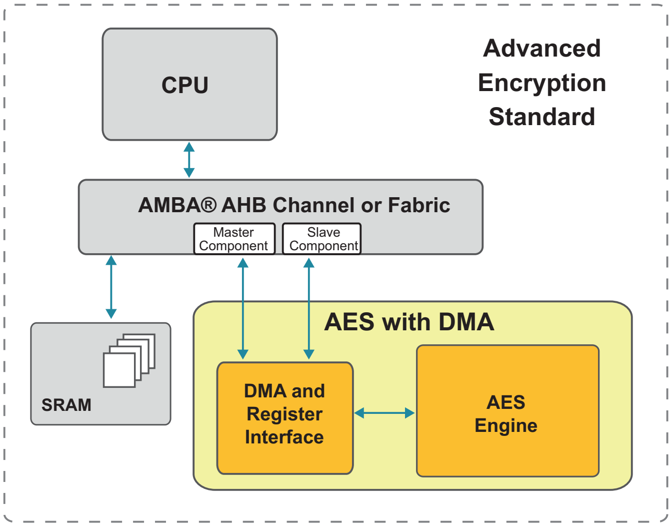
The AHB AES Encryption/Decryption Engine is a configurable core that interfaces to an AHB microprocessor bus. To accommodate a wide variety of system requirements, the Engine can be generated in one of three configurations: Low Gates, Mid Gates and High Gates.

The register interface of the AHB AES Engine is accessed via an AHB Slave component interface. Once the Engine has been configured and enabled, an AHB Master component interface is used to transfer data to/from system memory using DMA transfers. The core reads from a programmable source location in system memory into an internal Input FIFO, performs the desired action (encryption or decryption) on the data and stores the result in an internal Output FIFO. Lastly, the contents of the Output FIFO are written to a programmable destination location in system memory.

A maskable interrupt can be enabled to notify the processor when all DMA transfers are complete, and the output data has been transferred to system memory.

Features

- Advanced Encryption Standard FIPS 197 compliant
- Implements Rijndael algorithm
- Efficient "Tower Field" SBox implementation
- Encrypts / Decrypts 128 bit data blocks
- Supports key lengths of 128, 192, and 256 bits


Advanced Encryption Standard
CPU
AMBA® AHB Channel or Fabric
Master Component
Slave Component
SRAM
AES with DMA
DMA and Register Interface
AES Engine

- AHB Master component Interface for DMA memory transfers to and from the AES Engine
- AHB Slave component Interface for control/status register access
- AES Modes Supported
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Output Feedback (OFB)
- A maskable interrupt condition is supported
- Multiple AES Engine configurations
  - Low Gates (lowest gate count, slow performance)
  - Mid Gates (faster performance)
  - High Gates (highest performance)

Deliverables

- Verilog Source
- Complete Test Environment

For more information, please contact us at ip@silvaco.com.

SILVACO
HEADQUARTERS
4701 Patrick Henry Drive, Bldg #23
Santa Clara, CA 95054

Rev 012021_05
70122

NORTH AMERICA sales@silvaco.com
BRAZIL br_sales@silvaco.com
EUROPE eusales@silvaco.com

JAPAN jpsales@silvaco.com
KOREA krsales@silvaco.com
TAIWAN twsales@silvaco.com
SINGAPORE sgsales@silvaco.com
CHINA cn_sales@silvaco.com

WWW.SILVACO.COM