

# CAST

## AES-GCM

### GCM-AES Authenticated Encrypt/Decrypt Core

The AES-GCM core implements the GCM-AES authenticated encryption/decryption function, as specified in FIPS-197 Advanced Encryption Standard and in NIST's SP800-38D recommendation for GCM and GMAC.

The core can be programmed to either encrypt or decrypt 128-bit blocks of data, with a 128-bit, 192-bit or 256-bit cipher key. In addition a Hash value - the Tag - is calculated using the GHASH algorithm on the encrypted data or additional plaintext input. In decryption mode, the calculated TAG is compared with the TAG that accompanies the ciphertext, and a Fail or Pass flag is generated. The core has a 128-bit datapath and its throughput is one 128-bit block per 12/14/16 clock cycles (128/192/256-bit cipher key, respectively). The AES-GCM core supports 96-bit Initialization Vectors and input/output Tags of configurable length. A Key Expander is included for the AES-GCM core to automatically generate the AES Round Key Values.

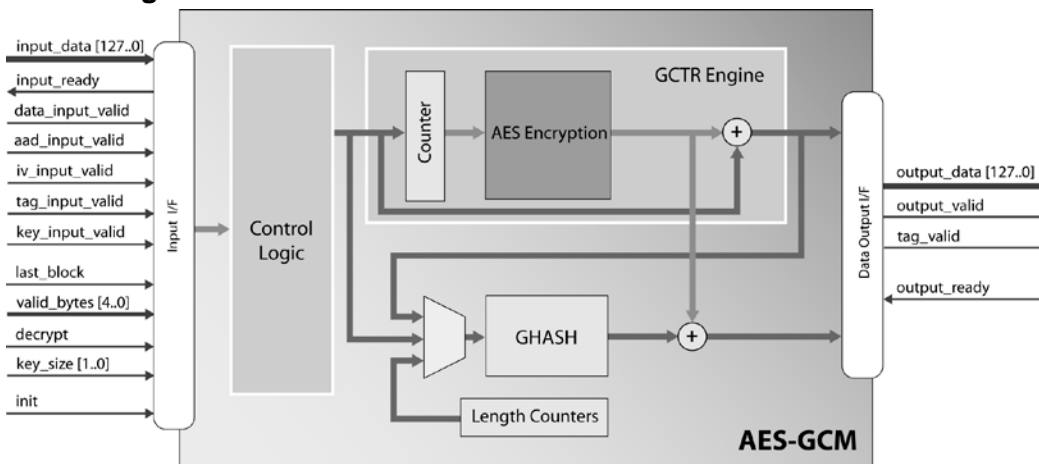
The AES-GCM core is equipped with easy to use fully stallable interfaces both for input and output. These are designed to permit the user's application to pause the produced output data stream when it is not able to receive data, or to pause the input stream towards the core according to data arrival rate.

The core has been verified against the SP800-38D Special Publication and the FIPS 197 standard using the Known Answer tests of the NIST AES-GCM Validation Suite (GCMVS). The core deliverables include these tests, plus a bit-accurate model (BAM) for generating additional test vectors. The AES-GCM core has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

## Applications

The AES-GCM core is suitable for a variety of applications, including: secure networking routers; wireless communications; encrypted data storage; secure video surveillance systems; and electronic financial transactions.

## Block Diagram



## Features

- Conforms to the Advanced Encryption Standard (AES) FIPS PUB 197 and NIST SP800-38D recommendation for GCM/GMAC
- Run-time programmable for encryption or decryption
- Processes each 128-bit block in 12/14/16 clock cycles for 128/192/256-bit cipher key, respectively
- Fully-stallable input and output interfaces, ideal for streaming applications, e.g. system software can:
  - pause input processing to match slow transmission, or
  - pause output processing to allow a slower application to catch up with decrypted data

### AES Features

- Supports 128/192/256-bit cipher key
- A Key Expander automatically generates and stores Round Keys for AES processing

### GCM Features

- 96-bit initialization vector
- GMAC operation supported. Additional Authenticated Data input, without encryption
- Input Tag verified against generated Tag during decryption
- 12 clocks per Hash operation

### General Features

- Robust verification environment includes simulation vector generation software
- Verified against the SP800-38D Special Publication and the FIPS 197 standard using the Known Answer tests of the NIST AES-GCM Validation Suite (GCMVS)
- Optimized design for ASIC or FPGA implementations
- Scan-ready design architecture

## Functional Description

Prior to any encryption or decryption operation, the cipher key must be programmed to the core. To save processing time and for simplicity of use, the Key Expander component is included and calculates the Round Key Values automatically. When the Key Expansion operation is complete, the user's application is signaled to provide the 96-bit Initialization Vector and the input data. The core accepts to the input, the plaintext to be encrypted, or the ciphertext to be decrypted, or plain data that will bypass the AES encryption and will only be Authenticated (Additional Authenticated Data). It is possible to pass only AAD, and no data for Encryption or decryption. In this case the core operates as a GMAC hash function.

The implementation of the GHASH operation requires only 12-clock cycles per 128-bit block, and is pipelined with the AES operations, thus the throughput of the core is determined by the throughput of AES operations, which is 12/14/16 clock cycles for 128/192/256-bit cipher keys, respectively. For example the core requires 12 clock cycles per 128-block of data encrypted / decrypted and authenticated, when processing an input stream with 128-bit cipher key.

The core features a powerful input / output interface, that permits fully stallable data streaming through the core. The application receiving the output of the core can pause output data generation arbitrarily. In a similar way, the application that feeds data to the input of the core can arbitrarily pause the data stream to it. The core can also stall the application to its input, when it is busy processing, or when the output cannot receive any more processed data.

The core can be configured before implementation to limit Tag length to be less than 128-bit.

## Export Permits

This encryption technology is governed internationally by export regulations. Immediate export of the core is permitted to the following countries for uses not related to weapons of mass destruction:

Argentina	Japan	South Korea
Australia	New Zealand	Switzerland
Canada	Norway	Turkey
European Union Member States	Russia	Ukraine
		United States

Please contact CAST to discuss delivery to other destinations; approval is subject to the applicable export licenses being granted. The license can be generated from either the EU or the USA. Please note that licensees are responsible for complying with the applicable requirements for re-export of electronics containing strong encryption technology.

## Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

## Verification

The core has been verified through extensive synthesis, place and route and simulation runs. It has also been embedded in several products, and is proven in FPGA technologies.

## Deliverables

The AES-GCM is available as a soft core (synthesizable HDL) for ASIC technologies and as a firm core (netlist) for FPGA technologies, and includes everything required for successful implementation. The ASIC version includes:

- HDL (VHDL or Verilog) RTL source code
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001)
- Software (C++) Bit-Accurate Model and test vector generator
- Synthesis scripts
- Simulation & synthesis scripts
- Comprehensive user documentation, including detailed specifications and a system integration guide