AES-GCM

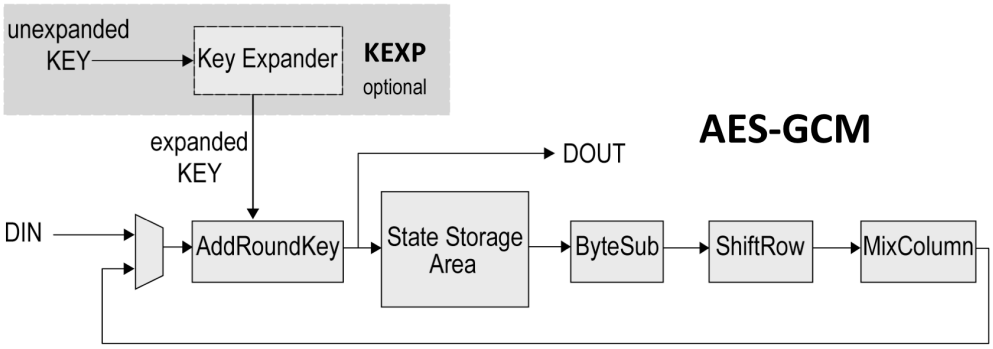
AES-GCM Authenticated Encrypt/Decrypt Core

The AES-GCM encryption IP core implements Rijndael encoding and decoding in compliance with the NIST Advanced Encryption Standard. It processes 128-bit blocks, and is programmable for 128-, 192-, and 256-bit key lengths.

Four architectural versions are available to suit system requirements. The **Standard** version (AES-GCM-S) is more compact, using a 32-bit datapath and requiring 44/52/60 clock cycles for each data block (128/192/256-bit cipher key, respectively). The **Fast** version (AES-GCM-F) achieves higher throughput using a 128-bit datapath and requiring 11/13/15 clock cycles for each data block depending on key size. For applications where throughput is critical there are two additional versions. The **High Throughput** AES-GCM-X can process 128 bits/cycle and the **Higher Throughput** AES-GCM-X2 can process 256 bits/cycle respectively independent of the key size.

GCM stands for Galois Counter. GCM is a generic authenticate-and-encrypt block cipher mode. A Galois Field (GF) multiplier/accumulator is utilized to generate an authentication tag while CTR (Counter) mode is used to encrypt.

Block Diagram



FEATURES

- Encrypts and decrypts using the AES Rijndael Block Cipher Algorithm
- NIST-Validated
- Implemented according to the National Institute of Standards and Technology (NIST) Special Publication 800-38D
- Processes 128-bit data in 32-bit blocks
- Employs user-programmable key size of 128, 192, or 256 bits
- Any size IV length
- Easy integration & implementation
  - Works with a pre-expanded key or can integrate the optional key expansion function
  - Fully synchronous, uses only the rising clock-edge, single-clock domain, no false or multicycle timing paths, scan-ready, LINT-clean, reusable design
  - Simple input and output interface, optionally bridged to AMBA™ interfaces or integrated with a DMA engine.
- Available in VHDL or Verilog source code format, or as a targeted FPGA

Applications

The AES-GCM can be utilized for a variety of encryption applications including protected network routers, electronic financial transactions, secure wireless communications, secure video surveillance systems, and encrypted data storage.

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.

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.

Key Expander

The AES algorithm requires an expanded key for encryption or decryption. The KEXP AES key expander core is available as an AES-GCM core option for the standard and fast versions. It is included for the higher throughput versions.

During encryption, the key expander can produce the expanded key on the fly while the AES core is consuming it. For decryption, though, the key must be pre-expanded and stored in an appropriate memory before being used by the AES core. This is because the core uses the expanded key backwards during decryption. In some cases a key expander is not required. This might be the case when the key does not need to be changed (and so it can be stored in its expanded form) or when the key does not change very often (and thus it can be expanded more slowly in software).

Implementation Results

The AES-GCM can be mapped to any AMD FPGA device (provided sufficient silicon resources are available). The following FPGA resources utilization and performance figures assume all core I/Os are routed on-chip. The throughput figures apply to the case that a 128-bit key is used.

AES-GCM Standard (-S)

Technology	Logic Resources	Memory Resources	Freq. (MHz)	Throughput (Mbps)
Kintex 7 (-3)	935 LUT	4 RAMB18	300	873
Virtex 7 (-3)	932 LUT	4 RAMB18	300	873
Kintex US (-3)	928 LUT	4 RAMB18	425	1,236
Kintex US+ (-3)	928 LUT	4 RAMB18	550	1,600
Versal (-2)	1,043 LUT	4 RAMB18	450	1,309
Zynq US+ (-1)	932 LUT	4 RAMB18	450	1,309

AES-GCM Fast (-F)

Technology	Logic Resources	Memory Resources	Freq. (MHz)	Throughput (Mbps)
Kintex 7 (-3)	1,746 LUT	8 RAMB18	250	2.909
Virtex 7 (-3)	1,742 LUT	8 RAMB18	250	2.909
Kintex US (-3)	1.697 LUT	8 RAMB18	375	4,364
Kintex US+ (-3)	1,735 LUT	8 RAMB18	475	5,527
Versal (-2)	1,660 LUT	8 RAMB18	400	4,655
Zynq US+ (-1)	1,681 LUT	8 RAMB18	375	4,364

AES-GCM High Throughput (-X)

Technology	Logic Resources	Memory Resources	Freq. (MHz)	Throughput (Gbps)
Kintex 7 (-3)	9,166 LUT	112 RAMB18	225	28.8
Virtex 7 (-3)	9,163 LUT	112 RAMB18	225	28.8
Kintex US (-3)	11,454 LUT	112 RAMB18	325	41.6
Kintex US+ (-3)	11,476 LUT	112 RAMB18	425	54.4
Versal (-2)	9,354 LUT	112 RAMB18	350	44.8
Zynq US+ (-1)	10,294 LUT	112 RAMB18	325	41.6

AES-GCM Higher Throughput (-X2)

Technology	Logic Resources	Memory Resources	Freq. (MHz)	Throughput (Gbps)
Kintex 7 (-3)	19,205 LUT	224 RAMB18	200	51.2
Virtex 7 (-3)	19,422 LUT	224 RAMB18	225	57.6
Kintex US (-3)	21,744 LUT	224 RAMB18	300	76.8
Kintex US+ (-3)	21,547 LUT	224 RAMB18	375	96.0
Versal (-2)	20,448 LUT	224 RAMB18	275	70.4

The provided figures do not represent the higher speed or smaller area for the core. Please contact CAST to get characterization data for your target configuration and technology.

Related Products

AES in CBC, CCM, CFB, CTR, ECB, LRW, OFB and XTS modes are also available as stand-alone cores.

AES-P: run-time programmable AES core supporting ECB, CBC, CFB, OFB and CTR modes.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.

Deliverables

The core is available in RTL (VHDL or Verilog) source code or as a targeted FPGA netlist. Its deliverable package includes the following:

- Sophisticated self-checking HDL Testbench
- C Model & test vector generator
- Sample simulation and synthesis scripts
- User documentation