The AES-GCM megafunction 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 megafunction 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 megafunction 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 megafunction supports 96-bit Initialization Vectors and input/output Tags of configurable length. A Key Expander is included for the AES-GCM megafunction to automatically generate the AES Round Key Values.

The AES-GCM megafunction 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 megafunction according to data arrival rate.

The megafunction 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 megafunction deliverables include these tests, plus a bit-accurate model (BAM) for generating additional test vectors. The AES-GCM megafunction has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs.

**Applications**

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

Prior to any encryption or decryption operation, the cipher key must be programmed to the megafunction. 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 megafunction 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 megafunction 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 megafunction 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 megafunction requires 12 clock cycles per 128-block of data encrypted / decrypted and authenticated, when processing an input stream with 128-bit cipher key.

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

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

Implementation Results

AES-GCM reference designs have been evaluated in a variety of technologies. The following are sample Altera results.

<table>
<thead>
<tr>
<th>Altera Device</th>
<th>LEs/ALUTs</th>
<th>Memory</th>
<th>DSP</th>
<th>I/Os</th>
<th>Fmax (MHz)</th>
<th>Quartus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyclone-IV</td>
<td>3,781</td>
<td>22 M9K</td>
<td>-</td>
<td>280</td>
<td>140</td>
<td>10.1</td>
</tr>
<tr>
<td>EP4CGX110-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Export Permits

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

Australia       Japan       Switzerland
Canada          New Zealand  United States
European Union  Norway      United States
Member 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 megafunction 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 megafunction 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 megafunction is available in ASIC (synthesizable HDL) and FPGA (netlist) forms, and includes everything required for successful implementation. The Altera version includes:

- Post-synthesis EDIF or NGC netlist
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001)
- Software (C++) Bit-Accurate Model and test vector generator
- Simulation scripts
- Place and route scripts
- Comprehensive user documentation, including detailed specifications and a system integration guide