AES GCM IP Core
Datasheet

November 2024

OVERVIEW

AES GCM IP Core is a Secure Symmetric Block Cipher IP Core that has compliance with the Advanced Encryption Standard (AES) specification in “FIPS 197”. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.

Countermeasures against side-channel attacks (DPA) are implemented in the AES IP Core. AES GCM IP Core is compatible with Xilinx FPGAs and INTEL FPGAs. VHDL is used as the Hardware Description Language of the IP Core. GCM mode of operations is supported and implemented according to “NIST SP800-38a” and “NIST SP800-38d”.

DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation
- AES Validation Suite Testbenches in SystemVerilog

FEATURES LIST

AES GCM IP Core:

- supports encryption and decryption for modes listed below:
  - *GCM mode of operation*
- supports offline and online key schedule.
- supports 128, 192 and 256-bit key lengths.
- has masked and non-masked modes.
- is compliant with FIPS 197.
- is tested on Z-7015 Z-7020 Z-7045
- has fully scalable input and output interfaces

LICENSING

IP can be licensed as;

- Single project license
- Multi-project license

Delivery type of the IP can be;

- Encrypted Netlist
- Encrypted RTL

MAINTENANCE & SUPPORT

First-year M&S is mandatory. Customers receive IP updates and phone and email support related to the IP core under the M&S agreement.

Technology Partner

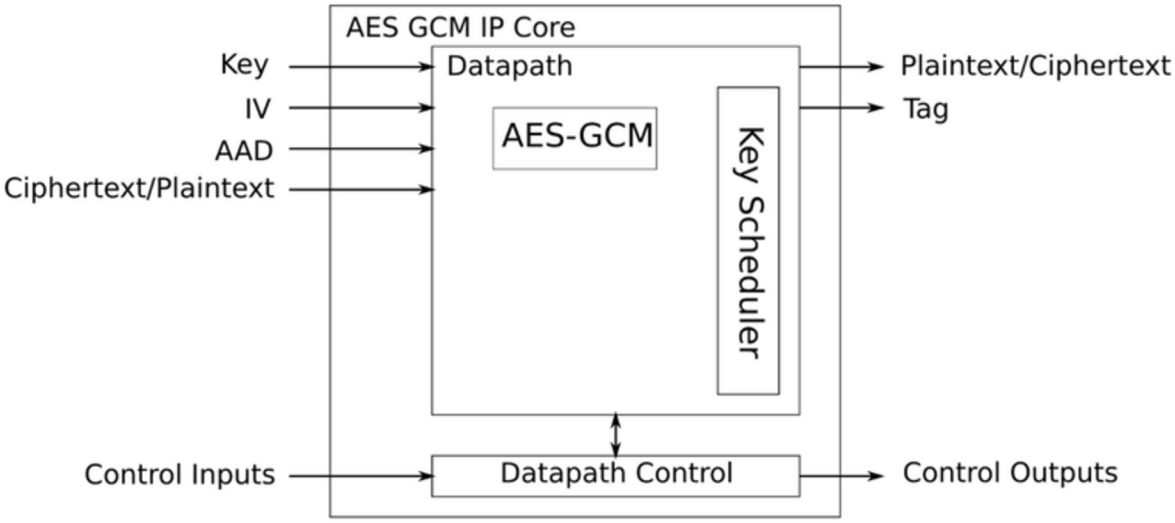
FPGA SYNTHESIS RESULTS

The FPGA resources requirements depend on the configuration.

Family/Device	Masked	LUT	FF	LUTRAM	Max. Freq.
Zynq/xc7z045ffg676-1	No	4695	1660	128	65 MHz
Zynq/xc7z045ffg676-1	Yes	7551	1794	128	166 MHz

Family/Device	Masked	ALM	FF	BRAM(M20K)	Max. Freq.
Aria10/10AS032E4F29I3SG	No	3921	1660	7	210 MHz
Aria10/10AS032E4F29I3SG	Yes	5561	1791	7	122 MHz

BLOCK DIAGRAM



Technology Partner