AES IP Core
Datasheet

November 2024

OVERVIEW

AES 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. Procenne AES IP Core is compatible with Xilinx FPGAs and INTEL FPGAs. VHDL is used as the Hardware Description Language of the IP Core. ECB, CBC, CTR, and GCM mode of operations are supported and implemented according to “NIST SP800-38a” and “NIST SP800-38d”.

FEATURES LIST

AES IP Core:

- supports encryption and decryption for modes listed below:
  - *ECB, CBC, CTR mode of operations*
  - *optional support for GCM*
- supports 128, 192 and 256-bit key lengths
- Side-channel protected (PCI v4.0 certified) and unprotected options are available
- is compliant with FIPS 197
- is tested on Xilinx Z-7015 Z-7020 Z-7045 FPGAs
- has fully scalable input and output interfaces

DELIVERABLES

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

LICENSING

IP can be licensed as;

- Single project license
- Multi-project license

Delivery type of the IP can be;

- Encrypted Netlist
- Encrypted RTL

ORDERING

Purchase order shall include the product number EIP-15009.

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

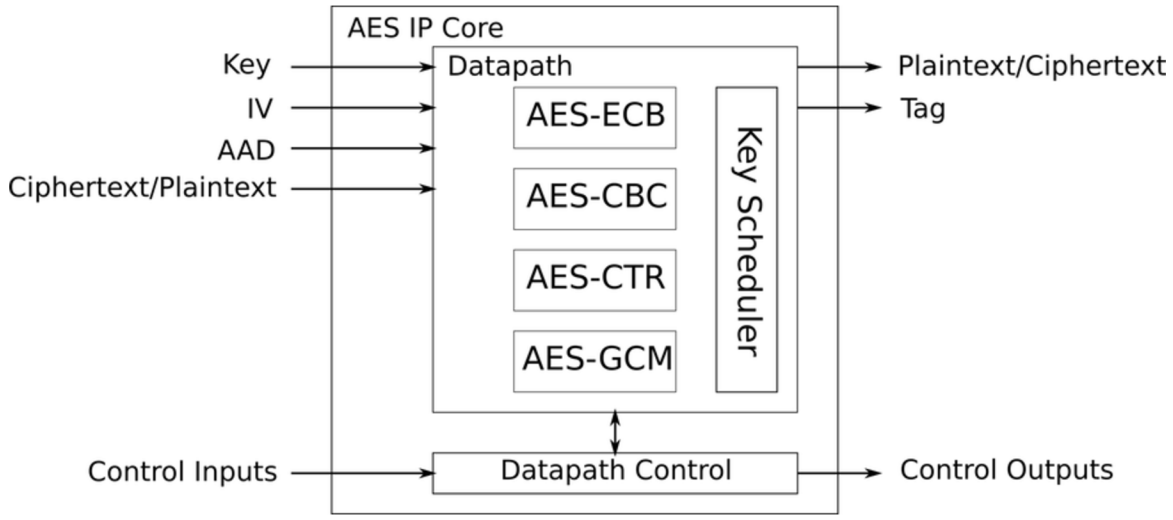
FPGA SYNTHESIS RESULTS

The FPGA resources requirements depend on the configuration.

Family/Device	Masked	GCM Mode	LUT	FF	LUTRAM	Max Clock Frequency on Z-7045 (speed grade -1)	Z-7045 FPGA-SoC TPS
Zynq/xc7z045ffg676-1	No	No	3665	929	128	220 MHz	~20M (ECB-128)
Zynq/xc7z045ffg676-1	Yes	No	6800	1067	128	220 MHz	~7.5M (ECB-128)
Zynq/xc7z045ffg676-1	No	Yes	6180	1792	128	220 MHz	~20M (ECB-128)
Zynq/xc7z045ffg676-1	Yes	Yes	9356	1925	128	220 MHz	~7.5M (ECB-128)

Family/Device	Masked	GCM Mode	ALM	FF	BRAM (M20K)
Aria10/10AS032E4F29I3SG	No	No	5926	800	7
Aria10/10AS032E4F29I3SG	Yes	No	5550	922	7
Aria10/10AS032E4F29I3SG	No	Yes	9620	1662	7
Aria10/10AS032E4F29I3SG	Yes	Yes	6961	1774	7

BLOCK DIAGRAM



Technology Partner