DATASHEET

Zyxx AES IP

Zyxx AES IP is an Intellectual Property implementing the AES *(Advanced Encryption Standard)* cryptographic algorithm. This algorithm was established as the standard encryption method by the U.S. National. Institute of Standards and Technology *(NIST)* in 2001, replacing the older Data Encryption Standard *(DES)*.

Key features :

Available in different configurations for 128, 192 and 256 bits :

- ECB
- CBC
- GCM
- CCM
- Full configuration for all modes above

Available in 3 versions :

- Ultra-Fast : very low latency and very high bandwith with higher footprint
- Fast : High bandwith with low latency and high frequency
- Small : Higher latency but smaller footprint

Full standard support :

Zyxx AES supports full specification of the AES standard.

AXI4 compatible interface can be added as an option for every configurations and versions

Available for a wide range of FPGA vendors :

AMD *(Xilinx)*, Intel *(Altera)*, Microchip, Lattice, Achronix, QuickLogic, and for ASICs.

Delivered as a netlist for the target required by the client.

V1.01

Results :

Devices	Resources*	Throughput *(ECB mode)*
Kintex Ultrascale +	6200 LUT	4.40 Gbps
Arria 2 GX	7050 LUT	3.70 Gbps
Polarfire	7600 LUT	2.45 Gbps

Table 1 : Resource usage
*(*Full configuration)*

CONTACT

ZYXX TECH 11, rue Planchat - 75020 Paris France

contact@zyxx.tech