DATASHEET

Zyxx Ascon IP

Zyxx Ascon IP is an Intellectual Property implementing the ASCON *(Authenticated Sponge CONstruction)* cryptographic algorithm in version 1.2. This algorithm has been selected by the NIST in the first phase of the process of standardization for lightweight cryptography.

Key features :

Available in different configurations :

- Ascon-128 for authenticated encryption with 64 bits data blocks
- Ascon-128a for authenticated encryption with 128 bits data blocks
- Ascon-80pq for authenticated encryption with 64 bits data blocks and 160 bits key
- Ascon-Hash for hashing with Ascon algorithm
- Ascon-Xof for extendable output function with Ascon algorithm
- 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 Ascon supports full specification of the Ascon standard selected by the NIST for lightweight cryptographic algorithm.

V1.02

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

Results :

Devices	Resources*	Throughput *(128a mode)*
Kintex Ultrascale +	4100 LUT	6.63 Gbps
Arria 2 GX	5050 LUT	3.30 Gbps
Polarfire	5400 LUT	3.00 Gbps

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

CONTACT

ZYXX TECH 11, rue Planchat - 75020 Paris France

contact@zyxx.tech