Zyxx Tech
Future relies on cryptography

Zyxx Ascon IP

Datasheet

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

- 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
- 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
- High bandwidth : Ultra Fast version can achieve 2.6 Gbps for Ascon-128a
- Small Footprint : Less than 2000 ALM on Cyclone 10 for the small version
- Delivered as a netlist for the target required by the client.

Contact
Zyxx Tech
11 rue Planchat
75020 Paris
France
contact@zyxx.tech