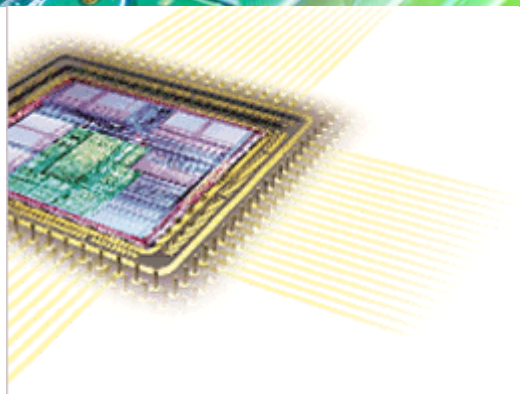
ntAES_XTS
XTS mode AES Processor

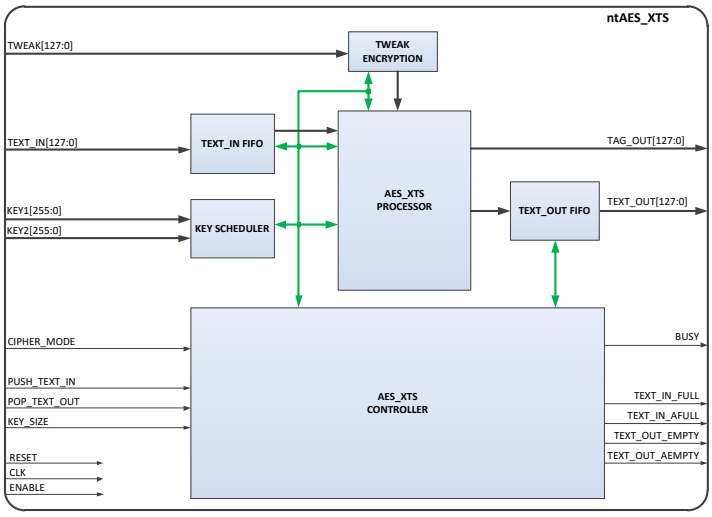


The ntAES_XTS IP Core is fully compliant with AES-XTS algorithm standardized at NIST SP800-38E and IEEE 1619-2007 recommendations targeting disk encryption applications at sector (data unit) addressable level. It is also known as a tweakable block cipher where the encryption process is controlled by the tweak a 128-bit value that is generated from the actual logical position of the data unit on the disk. This way identical data units stored at different places will result in different encrypted data thus addressing copy-and-paste attacks. Each data unit size is at least 128-bits. In addition each data unit size can be either an integral or non-integral number of 128-bit blocks. In case where the data unit size is not divisible with 128 then the ciphertext stealing procedure is used to enable correct encryption of the last block. Due to its highly parameterized and scalable architecture the users can trade off logic resources and performance in order to achieve optimum match with their application requirements. The implementation is low on latency, high speed with a simple interface for easy integration in SoC applications.

Applications

The ntAES_XTS core can be used in a variety of applications, including:

- Single SATA 2.0 Hard Disk Drives (up to 3 Gbps throughput rate)
- Single SATA 3.0 SSD (up to 6 Gbps throughput rate)
- USB 3.0 compliant storage
- Encrypted disk drives
- SSDs for server arrays (up to 64 Gbps typical throughput rate)
- Encrypted memory sticks



Features

- Supports high throughput AES XTS mode for data storage applications.
- Compliant with IEEE 1619-2007and NIST SP800-38E recommendations.
- Supports 128-bit data-path width.
- Supports 128 bit (XTS-256 mode) or 256-bit (XTS-512 mode) key sizes.
- Supports cipher stealing mode.
- Can be configured either as an encryptor or decryptor mode of operation.
- Provides a throughput rate of 16 Gbps at 125 MHz clock rate.
- Simple parallel user interface.
- Scalable architecture for optimal area/performance trade off.
- Fully synchronous design, using single clock.
- Portable to any ASIC or FPGA technology for a variety of applications.

Implementation results

The core has been targeted to both ASIC and FPGA technologies for various applications.
Noesis Technologies can also deliver netlist versions of the core optimized to specific area resources and performance requirements. Due to its scalable architecture optimum trade off between area and performance can be achieved.
Noesis Technologies will provide area and performance information on demand for our customers.

Deliverables

Noesis has engaged an "open" licensing philosophy in order to allow maximum technology transfer to our client's engineering teams and to facilitate the integration of our IP cores into our client's product. Various licensing models are available. The ntAES_XTS core is available as a soft core (synthesizable HDL) or as a firm core (netlist for FPGA technologies). The following deliverables are included:

- Fully commented synthesizable VHDL or Verilog source code or FPGA netlist.
- VHDL or Verilog test benches and example configuration files.
- Comprehensive technical documentation.
- Technical support.

Support

World-class technical support by phone or email is included. First year of maintenance is also included. Additional support and annual maintenance options are available.

Ordering information

To purchase or make any further inquiries about our ntAES_XTS core, or any other Noesis Technologies products or services, contact us at info@noesis-tech.com. Noesis Technologies products are purchased under a License Agreement, copies of which are available on request.

Noesis Technologies P.C.
Patras Science Park
Stadiou Rd, Platani Rion
GR-26504 - Patras
GREECE
Phone: +30 2610 911531
Email: info@noesis-tech.com